

EXHIBIT B

1
2 UNITED STATES DISTRICT COURT
3 SOUTHERN DISTRICT OF NEW YORK

4 -----X
5 SECURITIES AND EXCHANGE COMMISSION,

6 Plaintiff,
7 against

Civil Action No.
20-cv-1
(AT) (SN)

8 RIPPLE LABS, INC., BRADLEY
9 GARLINGHOUSE and CHRISTIAN A. LARSEN,

10 Defendants.
11 -----X

12 ** HIGHLY CONFIDENTIAL **
13
14
15
16
17
18
19
20
21
22

23 VIDEOTAPED DEPOSITION OF [REDACTED] Ph.D.

24 New York, New York

25 Friday, December 17, 2021

Reported by

JEFFREY BENZ, CRR, RMR

JOB NO. 203725

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

December 17, 2021

8:21 a.m.

Videotaped Deposition of [REDACTED]
Ph.D., held at the offices of the U.S. Securities
and Exchange Commission, 200 Vesey Street, New
York, New York, before Jeffrey Benz, a Certified
Realtime Reporter, Registered Merit Reporter and
Notary Public of the State of New York.

A P P E A R A N C E S:

U.S. SECURITIES AND EXCHANGE COMMISSION

Attorneys for Plaintiff

200 Vesey Street

New York, New York 10281

BY: MARK SYLVESTER, ESQ.

JON DANIELS, ESQ.

LADAN STEWART, ESQ. (Remotely)

DAPHNA WAXMAN, ESQ.

A P P E A R A N C E S: (Ctd.)

DEBEVOISE & PLIMPTON LLP

Attorneys for Defendant Ripple Labs, Inc.

919 Third Avenue

New York, New York 10022

LISA ZORNBERG, ESQ.

ASHLEY HAHN, ESQ. (Remotely)

BENJAMIN LEB, ESQ. (Remotely)

SCOTT CARAVELLO, ESQ. (Remotely)

CHRISTOPHER FORD, ESQ.

-and-

KELLOGG, HANSEN, TODD, FIGEL & FREDERICK

1615 M Street, N.W.

Washington, D.C. 20036

BY: COLLIN WHITE, ESQ.

A P P E A R A N C E S: (Ctd.)

PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP

Attorneys for Defendant Christian Larsen

1285 Avenue of the Americas

New York, New York 10019

BY: CARLY LAGROTTERIA, ESQ.

MEREDITH DEARBORN, ESQ. (Remotely)

CLEARY GOTTlieb STEEN & HAMILTON LLP

Attorneys for Defendant Bradley Garlinghouse

One Liberty Plaza

New York, New York 10006

BY: SAMUEL LEVANDER, ESQ.

ALSO PRESENT:

CHRISTOPHER JOHNSON, Videographer

DAVID SCHWARTZ, Ripple Labs, Inc. (Remotely)

DEBORAH McCRIMMON, Ripple Labs, Inc. (Remotely)

STELLA UVAYDOVA, S.E.C. (Remotely)

KYLE E. CHERMAK, Debevoise & Plimpton (Remotely)

1 [REDACTED] - Highly Confidential

2 THE VIDEOGRAPHER: We are now on the
3 record. This is the start of media labeled
4 number 1 of the video-recorded deposition
5 of [REDACTED] in the matter of
6 Securities and Exchange Commission versus
7 Ripple Labs, Incorporated, et al., in the
8 United States District Court for the
9 Southern District of New York. Civil
10 Action Number 20-CV-10832 (AT) (SN).

11 This deposition is being held at
12 U.S. SEC, 200 Vesey Street, Suite 400,
13 New York, New York. Today is Friday,
14 December 17, 2021. And the time on the
15 video monitor is approximately 8:21 a.m.
16 My name is Chris Johnson. I am the legal
17 video specialist from TSG Reporting,
18 Incorporated, headquartered -- excuse me.

19 The court reporter today is Jeff Benz,
20 in association with TSG Reporting.

21 Will all counsel present please
22 introduce yourself and the parties you
23 represent.

24 MS. ZORNBERG: Good morning. I'm Lisa
25 Zornberg from Debevoise & Plimpton together

1 [REDACTED] - Highly Confidential

2 with Chris Ford, who is also in the room.

3 We represent Defendant Ripple Labs, Inc.,
4 in this case.

5 I would also just let you know that we
6 have through Webex participating today two
7 employees of Ripple: David Schwartz, who
8 is the chief technology officer, and
9 Deborah McCrimmon, who is the vice
10 president for litigation.

11 THE WITNESS: Good morning.

12 MR. SYLVESTER: I'm Mark Sylvester. I
13 am an attorney for the plaintiff, the
14 Securities and Exchange Commission. I'm
15 here with my colleagues Jon Daniels and
16 Daphna Waxman.

17 MR. LEVANDER: Samuel Levander of
18 Cleary Gottlieb, on behalf of the defendant
19 Brad Garlinghouse.

20 MS. LAGROTTERIA: Carly Lagrotteria.
21 I'm from Paul, Weiss.

22 THE VIDEOGRAPHER: Will the court
23 reporter please swear in the witness and
24 then we may proceed.

25

1 [REDACTED] - Highly Confidential

2 [REDACTED] Ph.D.,

3 called as a witness, having been first
4 duly sworn by Jeffrey Benz, a Notary
5 Public within and for the State of
6 New York, was examined and testified as
7 follows:

8 EXAMINATION BY MS. ZORNBERG:

9 Q. Good morning.

10 A. Good morning.

11 Q. Dr. [REDACTED] for purposes of today's
12 deposition, I'm going to refer to Defendant
13 Ripple Labs as Ripple. Okay?

14 A. Very good, yes.

15 Q. Yes? Okay. Are you taking any
16 medication or suffering from any medical or
17 physical condition, that would prevent you from
18 testifying truthfully and completely today?

19 A. No.

20 Q. Okay. Please state your full name for
21 the record.

22 A. [REDACTED]

23 Q. Where do you live?

24 A. I live in [REDACTED].

25 Q. How old are you?

1 [REDACTED] - Highly Confidential

2 A. 44.

3 Q. Have you ever been deposed before?

4 A. No.

5 Q. Okay. You understand that your
6 testimony is under oath. Correct?

7 A. Yes.

8 Q. And it's being taken down by the
9 stenographer and by the videographer in this
10 lawsuit. You understand that --

11 A. Yes.

12 Q. -- correct?

13 A. Yes. I do.

14 MR. SYLVESTER: Just let her finish
15 the question before you answer.

16 THE WITNESS: Okay.

17 MS. ZORNBERG: Just a couple of ground
18 rules. Because the court reporter is
19 taking down all of the testimony, it's
20 important that you verbalize all answers.
21 So a nod of the head is not sufficient.
22 You have to be verbal.

23 Another ground rule that your counsel
24 just pointed out -- or not -- counsel for
25 the SEC just pointed out, please let me

1 [REDACTED] - Highly Confidential

2 finish my questions before you start to
3 give an answer so that we get a clean
4 record and we're not talking over one
5 another.

6 Sound good?

7 A. Yes.

8 Q. Okay.

9 We'll take regular breaks. If you
10 need a break at any point, just let me know and
11 we'll be accommodating.

12 The only thing I may ask is that you
13 answer a pending question before we take a
14 break.

15 Okay?

16 A. Yes.

17 Q. Okay. Is English your first language?

18 A. No.

19 Q. What is your first language?

20 A. [REDACTED].

21 Q. Are you fluent in English?

22 A. I consider myself fluent in English,
23 yes.

24 Q. Do you write papers in English?

25 A. I do.

1 [REDACTED] - Highly Confidential

2 Q. Have you taught classes in English?

3 A. Yes, I did.

4 Q. Okay. If for whatever reason you
5 don't understand a question, that I've asked,
6 please let me know you don't understand the
7 question. I'll be happy to repeat it or
8 rephrase it.

9 Have you ever lived in the
10 United States, Dr. [REDACTED]

11 A. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

15 Q. Have you ever given testimony under
16 oath in any type case?

17 A. I did in [REDACTED].

18 Q. What type of case?

19 A. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

1 [REDACTED] - Highly Confidential

2 Q. [REDACTED]

4 Q. I'm sorry for that experience.

5 Have you ever served as an expert
6 witness in any type of case before?

7 A. You mean the court case, such as this
8 one, the legal proceeding?

9 Q. Yes, in a legal proceeding.

10 A. No, I did not. No.

11 Q. Okay. So this case is the first time
12 that you're serving as an expert in any type of
13 legal case.

14 A. Yes, it is.

15 Q. When was your first contact with the
16 SEC about this case?

17 A. My first contact with the SEC in this
18 case was in the summer, so June this year.

19 Q. Your first contact from the SEC was
20 June 2021?

21 A. 2021. June 2021.

22 Q. How did that contact come about? I'm
23 not asking you to tell me your conversations
24 with SEC lawyers, but how did -- without
25 revealing those conversations, how did the

1 [REDACTED] - Highly Confidential

2 contact come about?

3 A. [REDACTED] people from [REDACTED]
4 reached out to me, so they found me. I think it
5 was a cold email first. Would I be interested
6 in -- I think the email said, I believe, I --
7 the email said the -- the -- like, they would
8 like me to be an expert on some -- on some court
9 case related to the blockchain.

10 Then I had a discussion with [REDACTED]
11 with maybe one hour, initial, where they didn't
12 reveal which case this was.

13 And, after that, I had a call with
14 SEC, which was also -- so we were all talking
15 early June. I could not give you exact dates,
16 but we are talking early June.

17 Q. When was -- when was the cold email
18 from [REDACTED] that initial email from [REDACTED]

19 A. Let's say it was, again, early June or
20 very late May, I would put more probability -- I
21 don't know. I cannot vouch for it. My take is
22 very early June. We're talking 1st to 4th of
23 June maybe. I'm not sure.

24 Q. Was that your first contact with

25 [REDACTED]

1 [REDACTED] - Highly Confidential

2 A. Yes.

3 Q. What is [REDACTED]

4 A. I believe it's -- so it's a litigation
5 firm that, to my understanding, helps SEC with
6 certain case.

7 Q. Is your engagement in this case the
8 first time you've ever interacted with [REDACTED]

9 A. Yes, it is.

10 Q. Who at [REDACTED] did you speak with
11 prior to your engagement in this case?

12 A. I spoke to [REDACTED]. I'm not sure I
13 pronounce his name correct. I spoke to
14 [REDACTED] and [REDACTED]. I believe that is
15 it.

16 Q. Can you give the last name one more
17 time?

18 A. [REDACTED].

19 Q. [REDACTED]?

20 A. Yes.

21 Q. Okay. Thank you.

22 A. [REDACTED] and [REDACTED], I think, is
23 the last name.

24 Q. Can you describe your communications
25 with [REDACTED] about this case.

1 [REDACTED] - Highly Confidential

2 A. [REDACTED] reached out to me. And,
3 again, if I recall correctly, to the best of my
4 recollection, he was trying to understand if I
5 would like to be an expert in a certain
6 litigation in a court case. Since it related to
7 blockchain, I'm interested. But I'm not
8 necessarily interested in just picking up
9 anything, so -- you know.

10 Then he suggested that -- he asked me
11 few questions about, how would you -- how would
12 you think about going classifying certain
13 blockchain system as decentralized and
14 centralized? So we discussed that topic.

15 And I told him, basically, what's my
16 approach, how I think about it. So we talked
17 about it real time, so I didn't -- he was asking
18 questions; I was giving him answers.

19 And, yeah. I guess this was the
20 reason they carried on with me.

21 Q. That was -- that was your initial
22 one-hour call, was with [REDACTED]

23 A. There might be [REDACTED] on that call
24 and [REDACTED] but, yeah. So the first --
25 I -- I distinctly remember communicating -- like

1 [REDACTED] - Highly Confidential
2 discussing this decentralization/centralization
3 with [REDACTED].

4 Q. How did you discuss the issue with
5 decentralization with [REDACTED] In other
6 words, was it a phone call, a video conference,
7 an email, some other messaging communications?

8 A. It was a video call or Webex, I
9 believe.

10 Q. And did you email with him as well
11 about the subject of decentralization?

12 A. I don't recall I did.

13 Q. Is it possible you did?

14 A. I doubt. It might be possible since I
15 don't recall for sure. So let's leave it to
16 possibility, I doubt.

17 Q. Have you communicated with
18 [REDACTED] by any means other than -- in
19 writing, by any means other than email?

20 A. In writing an email or sending an
21 email? No?

22 THE COURT REPORTER: I'm sorry. Say
23 that again, please.

24 A. I'm just repeating the question.
25 Sorry. So -- have you communicated in writing?

1 [REDACTED] - Highly Confidential

2 I'm repeating the question.

3 Q. Yes.

4 A. In any other means other than email?

5 No. Could I be missing something?

6 Like -- we didn't text. We didn't write
7 letters, so no.

8 Q. Okay. So -- did [REDACTED] tell you
9 what he was looking for?

10 MR. SYLVESTER: Objection.

11 Q. You can answer.

12 A. I can answer. Okay.

13 No. No.

14 Q. Other than this case, have you worked
15 with the SEC in any capacity?

16 A. No.

17 Q. Prior to -- do you have a written
18 retention agreement in this matter with the SEC?

19 A. I have a written agreement with

20 [REDACTED] And with SEC, I -- I signed some
21 documents which are nondisclosure documents
22 and -- and certain documents. I think, for
23 example, things like my rate and these things,
24 they are all signed with [REDACTED]

25 Q. Okay. Do you know --

1 [REDACTED] - Highly Confidential

2 A. I don't know if this answers your
3 question.

4 Q. Do you know the date of your retention
5 agreement with [REDACTED]

6 A. It was -- it must be, again, in June.
7 I don't know the date.

8 Q. Okay. Prior to your engagement in
9 this case, had you heard of Ripple Labs, Inc.?

10 A. I did. Yes.

11 Q. How?

12 A. I followed the blockchain space since
13 2009, so basically since the inception of
14 bitcoin. And Ripple was definitely prominent
15 blockchain network, which on top of that was
16 trying to put in work, consensus protocols that
17 are different than those used by bitcoin, which
18 I happened to be researching since 2003. So
19 again, much before -- like considerably before
20 bitcoin was accepted -- incepted.

21 So I did research on these protocols
22 in my Ph.D. thesis. Since I did it and Ripple
23 was essentially trying to come up with a
24 similar, let's say the protocol which falls
25 into -- into this category, then it obviously

1 [REDACTED] - Highly Confidential

2 drew my attention.

3 And then I was paying attention to the
4 protocol discussing at that time with my
5 colleague and collaborator, [REDACTED],

[REDACTED].

7 And then we discussed, like, look at
8 this protocol; this is similar to what we did.
9 But it doesn't seem that -- you know, there
10 seems to be something not correct with this
11 protocol. And then we actually started looking
12 into that.

13 And then I understood that Ripple -- I
14 think at some point Ripple was in the name of
15 the network. Before it was called XRP Ledger,
16 there were different names. And Ripple was in
17 the name of the network. And then the name of
18 the Ripple was associated to this organization,
19 this -- this protocol, as --

20 Q. So when -- approximately when did you
21 start talking to your collaborator, [REDACTED],
22 about the protocol for the XRP Ledger?

23 A. We started intensively -- we might
24 have mentioned it before the date I will give
25 you, but we started looking -- actually, he

1 [REDACTED] - Highly Confidential

2 started looking into more details, and I was
3 following on the high level -- I can explain in
4 more technical details what's the high level --
5 in 2015.

6 Q. Okay. So --

7 A. I heard about -- sorry. Just to the
8 complement the answer, I heard about Ripple even
9 before, as you're -- as I'm following the --

10 Q. Yeah.

11 A. Yeah.

12 Q. So let me just clarify. You heard
13 about Ripple prior to 2015, correct?

14 A. Yes.

15 Q. The person you've described as your
16 collaborator, [REDACTED], started looking at the
17 protocol for the XRP Ledger, around 2015?

18 A. So 2015 I moved back to [REDACTED], as
19 you can see in my CV. Right? So this is the
20 moment when I was collaborating with [REDACTED]
21 nonstop. So I was collaborating with [REDACTED]
22 since 2008 to 2010 when I was in [REDACTED]. And then
23 I went to [REDACTED] to be assistant professor. But
24 we continued collaboration. So we might have
25 mentioned it before, but, intensively, we

1 [REDACTED] - Highly Confidential

2 started looking into it in 2015.

3 Q. You just said that you and [REDACTED]
4 intensively started looking at the XRP Ledger
5 protocol in 2015.

6 A. Uh-huh.

7 Q. But a few minutes ago, you said that
8 [REDACTED] started looking at it first, and you
9 were following his work at a high level.

10 Can you clarify?

11 A. Yes. It's the first thing. So when I
12 say "we," I mean as a team, because we looked --
13 but he was leading the analysis of the -- let's
14 say within the team, he was leading the analysis
15 of the XRP Ledger.

16 I was following it on a high level. I
17 can explain. For -- yeah. If you wish.

18 Q. What does it mean that you and [REDACTED]
19 were the team?

20 A. We co-authored many scientific papers
21 together. We would discuss protocol -- when we
22 designed a new protocol, we would discuss
23 protocol details together, each and every one of
24 us trying to find, you know, shortcomings in
25 others' work. And this is what, you know, the

1 [REDACTED] - Highly Confidential

2 whole scientific community is doing. We're just
3 at a faster pace of iteration, talking to each
4 other.

5 We're exchanging ideas, collaborating
6 on -- on building protocols, collaborating on
7 analysis of the protocols and so on.

8 Q. Okay.

9 And so just to make sure I understand
10 your testimony, [REDACTED] started looking into
11 the details of the XRP Ledger protocol in 2015?

12 A. To my understanding, yes. He might
13 have started earlier. But at least in 2015.

14 Q. Was that as part of his work at
15 [REDACTED] or as a separate interest of his?

16 MR. SYLVESTER: Objection.

17 Q. You can answer.

18 A. Uh-huh. As part of -- so we had -- we
19 had very much freedom in what we choose to work
20 for [REDACTED]. It was never -- as researchers of the
21 standing that we were just, just like how -- how
22 [REDACTED] approached blockchain. They let us suggest
23 what are we going to work on.

24 So, yes, it was part of [REDACTED].
25 But it came -- you can say that it came bottom

1 [REDACTED] - Highly Confidential

2 up, grassroots, during -- because of his
3 interest, because he thought it is relevant.

4 Q. So can you please describe what work
5 you personally have done, or did, relating to
6 the XRP Ledger protocol, while at [REDACTED].

7 A. So I looked at the -- the -- the
8 original white paper. And basically, original
9 white paper, which is co-authored by David
10 Schwartz, had reasoned about the quorums, which
11 are the sizes of the faulty nodes, Byzantine
12 faulty nodes that are tolerated by the protocol.
13 And these were rather nonstandard.

14 Since the protocol was underspecified,
15 I didn't dive much into the details. But it
16 seemed that this is not a correct protocol, so
17 it's not doing what it promises to do. So I was
18 reading and I was gathering this understanding.

19 Q. So let me pause you there.

20 A. Yes.

21 Q. In what year was this?

22 A. This is year 2015.

23 Q. Okay. Can you just state again,
24 what -- what was it that you, based on reading
25 the white paper by David Schwartz, did you think

1 [REDACTED] - Highly Confidential

2 was not correct?

3 A. It was not correct that it can
4 basically tolerate -- it can provide a guarantee
5 that it does.

6 Q. Which guarantees did you felt, based
7 on reading the white paper, the XRP Ledger
8 protocol could not provide?

9 A. It -- that it couldn't provide safety
10 and liveness because of the way quorums are
11 sized, essentially, in the protocol.

12 Q. What does it mean for a quorum to be
13 sized?

14 A. Because of its assumption in the
15 number of quorums and the assumption of the
16 number of correct nodes, the number of faulty
17 nodes. So that defines the quorums. So the
18 adversarial assumption is how many -- which
19 percentage of nodes can be Byzantine or not. So
20 basically the -- how the protocol was
21 constructed, it was intuitive, according to my
22 prior experience of designing this protocol,
23 that something is wrong here.

24 Q. Did you write any papers between 2015
25 and 2020 relating to your evaluation of the

1 [REDACTED] - Highly Confidential

2 XRP Ledger protocol?

3 A. So we write -- so [REDACTED] we wrote
4 one paper, which is called [REDACTED]

[REDACTED] where, basically, the things with
6 Ripple protocols were mentioned. So --

7 Q. Other than that paper you've
8 mentioned, [REDACTED] --

9 A. Yes.

10 Q. -- did you write -- in which you --
11 you said that the XRP Ledger protocol is
12 mentioned in there. Correct?

13 A. Yes.

14 Q. Did you -- did that paper, [REDACTED]
[REDACTED] express or contain
16 analysis of safety and liveness concerns that
17 you're talking about here today?

18 A. I believe -- I believe we mentioned
19 it. But it was not analyzed in the details, for
20 example, at the level I'm giving in the -- in my
21 expert report.

22 Q. Other than the paper [REDACTED]
[REDACTED] have you written any
24 papers to date addressing the XRP Ledger
25 protocol?

1 [REDACTED] - Highly Confidential

2 A. No, I did not.

3 Q. So the answer is, no?

4 A. No.

5 Q. Within [REDACTED], did you prepare
6 any written analysis, during the time that you
7 were at [REDACTED], on the XRP Ledger
8 protocol?

9 A. No, I did not.

10 Q. Do you know anyone who works for
11 Ripple?

12 A. You mean like personally?

13 Q. Yes.

14 A. I do not, no.

15 Q. Have you ever met Chris Larsen?

16 A. No, I did not.

17 Q. Have you ever met Jed McCaleb?

18 A. No, I did not.

19 Q. Have you met David Schwartz?

20 A. No, I did not.

21 Q. Have you ever communicated with
22 David Schwartz in any way?

23 A. No, I did not.

24 Q. Back in 2015 when you've described
25 that you started looking at the XRP Ledger

1 [REDACTED] - Highly Confidential

2 protocol, did you ever consider reaching out to
3 David Schwartz to discuss your concerns about
4 the protocol?

5 A. No, I did not.

6 Q. Why not?

7 A. You know, we were focusing -- it's in
8 our interest to look at other protocols. At
9 that time we were trying to build -- we were
10 busy building our own systems. And it's not my
11 job to help others, necessarily. I didn't have
12 a -- you know, even this -- the attack was not
13 specific or anything. And it's not my job to
14 reach out to people and help them out.

15 Q. What do you mean -- just said the
16 attack was not specific or anything.

17 A. So --

18 Q. What do you mean by that?

19 A. Yeah. So, for example, the attack
20 that I'm describing in my report, I didn't have
21 that level of understanding of Ripple protocol
22 that I gained later on, where I actually took to
23 analyze it in details, took the task of
24 analyzing it in details.

25 Q. When was it that you analyzed the

1 [REDACTED] - Highly Confidential

2 protocol at the level of detail that you're
3 describing is contained in your report?

4 A. After I -- after I was retained by
5 [REDACTED] and I started working for SEC, so we're
6 talking after June this year.

7 Q. Would it be fair to say that the
8 concerns that you noted in 2015 about the
9 XRP Ledger protocol were at a high level?

10 MR. SYLVESTER: Objection.

11 Q. You can answer.

12 A. We can say that, yes.

13 Q. And it was not until after -- sometime
14 in or after June 2021 that you looked at those
15 issues in detail. Correct?

16 A. Yes.

17 Q. Have you ever met Brad Garlinghouse?

18 A. No.

19 Q. Have you ever spoken to anyone at
20 Ripple, to your knowledge?

21 A. No.

22 Q. Did you read any of the deposition
23 transcripts taken in this case?

24 A. I did.

25 Q. Which ones?

1 [REDACTED] - Highly Confidential

2 A. David Schwartz.

3 Q. How many transcripts of David
4 Schwartz's testimony did you read?

5 A. I'm not sure I get the question. How
6 many?

7 Q. Do you know if there's one or more
8 than one deposition or -- let me rephrase. Do
9 you know if there's one or more than one
10 transcript of David Schwartz giving testimony
11 related to this case?

12 A. To my understanding, there is one.

13 Q. Okay. So you read one transcript?

14 A. One.

15 Q. Did you read the entire transcript?

16 A. I did.

17 Q. All right. Do you recall the date of
18 the transcript that you read?

19 A. The transcript. I think it was in
20 May. Don't hold my -- you know. I think it was
21 May, May this year.

22 Q. Dr. [REDACTED] do you know anyone from
23 the Ethereum Foundation?

24 A. No.

25 So let me put it this way: I never

1 [REDACTED] - Highly Confidential

2 met physically anyone.

3 So, no, if this is like your
4 definition of "no," no, we never met physically
5 or something.

6 Q. Have you ever -- have you ever met in
7 any way, physically or through other means of
8 communication, Vitalik Buterin?

9 A. No, I did not.

10 Q. Have you ever met in any way
11 Gavin Wood?

12 A. No, I did not.

13 Q. Do you know who he is?

14 A. I know.

15 Q. Who is he?

16 A. He's the -- one of the original
17 founders of Ethereum.

18 Q. Okay.

19 A. And currently, he is mostly involved
20 in the Polkadot project, so he's putting his
21 attention there.

22 Q. What is the relationship between
23 Ethereum Foundation and Ether, if you know?

24 A. I would need more details to answer
25 this question. So Ether -- yeah, I would need

1 [REDACTED] - Highly Confidential

2 more details to answer this question. So
3 normally Ether is the token which is the native
4 token of Ethereum network. And Ethereum
5 Foundation is linked to the development of
6 Ethereum network, so that's it.

7 Q. Do you know what Ethereum Foundation
8 does?

9 A. To my understanding, it funds the
10 development of the Ethereum network. It might
11 be doing other things that I'm not aware.

12 Q. Do you know what the Ethereum
13 Foundation's ecosystem support program is?

14 A. I do not.

15 Q. Does the existence of a foundation
16 that's dedicated to supporting the Ethereum
17 network mean that Ethereum is a centralized
18 system?

19 MR. SYLVESTER: Objection.

20 Q. You can answer.

21 A. No, it does not. So it's -- I give
22 definitions in my report. I give precise
23 definitions, about the basic or minimal
24 condition for a system to be considered
25 decentralized. I can repeat it for you if you

1 [REDACTED] - Highly Confidential

2 wish.

3 And the existence of Ethereum
4 Foundation is related to governance aspect that
5 I discussed my report. It should be looked at
6 as such, through this lens.

7 Q. Is it your view that simply the
8 existence of a foundation that is dedicated to
9 supporting development on a particular
10 blockchain network, does that automatically mean
11 that network is centralized?

12 A. It does not. So I could imagine
13 several -- so imaginary networks, several people
14 who are interested in development of a
15 blockchain network, they come up with their own
16 foundations. So you could have ten foundations
17 for one blockchain network.

18 And, yeah, we call it centralized
19 because these foundations exist, so normally
20 these -- these would be people who distribute
21 their wealth, let's say, in those tokens, to
22 fund the development of the network.

23 Q. That does not render the network
24 centralized.

25 MR. SYLVESTER: Objection.

1 [REDACTED] - Highly Confidential

2 A. So that -- that meaning what? Can you
3 repeat? "That does not render" -- so "that" is
4 what?

5 Q. I'm just trying to clarify my own
6 understanding of what you're saying. Does the
7 mere existence of one or more foundations,
8 dedicated to supporting a blockchain network,
9 mean that network is centralized?

10 A. You got my brain racked. So does
11 the -- I'm repeating the question. Does the
12 existence of several foundations mean that the
13 blockchain network is centralized?

14 I guess the answer is no.

15 So. Yeah.

16 Q. In the case of Ethereum, besides the
17 Ethereum Foundation, are you aware of other
18 foundations that -- that exist in order to
19 support Ethereum?

20 MR. SYLVESTER: Objection.

21 A. To support Ethereum development, to
22 support --

23 Q. Yes.

24 A. To support --

25 I'm not aware of any.

1 [REDACTED] - Highly Confidential

2 Q. Okay. Do you know anyone from
3 ConsenSys?

4 A. No, I do not.

5 Q. Have you ever met Joe Lubin?

6 A. No.

7 Q. Do you know what ConsenSys does?

8 A. ConsenSys, to my understanding, it
9 takes the Ethereum public blockchain network and
10 tries to adopt it in a way that it can be used
11 in so-called permission blockchain networks, in
12 blockchain for businesses, as we call it in [REDACTED]

13 And I know about the existence of
14 ConsenSys because they were, like, competitors
15 to [REDACTED] once we worked in [REDACTED] the permission
16 blockchain space, because they were trying to
17 build their technology on the Ethereum stack.
18 That's what I know about ConsenSys.

19 Q. Okay. Do you know anyone from the
20 Bitcoin Foundation.

21 A. No.

22 Q. Have you ever met Gavin Andresen?

23 A. "Andresen."

24 No.

25 Q. Andresen.

1 [REDACTED] - Highly Confidential

2 Have you ever met someone named
3 Craig Wraight?

4 A. No, I did not.

5 Q. Do you believe that he invented
6 bitcoin?

7 A. No, I do not.

8 Q. Why not?

9 A. There is a simple proof. If you
10 invented bitcoin and you claim you did it, there
11 is an, arguably, high probability that you mined
12 as an early player in the bitcoin network one
13 the first bitcoin blocks.

14 So if you want to prove, it's very
15 easy. So you could use the cryptographic keys
16 that are associated with that block to sign
17 basically any message. So you give the Craig
18 Wraight challenge: Sign me this message. And
19 if he does it, you can verify that this was
20 signed with the keys that belonged to one of the
21 first blocks.

22 That's a very simple test. And he
23 never was able to produce such a test -- to
24 basically produce such a signature.

25 Q. Do you know what services the Bitcoin

1 [REDACTED] - Highly Confidential

2 Foundation provides to bitcoin?

3 MR. SYLVESTER: Objection.

4 A. I do not.

5 Q. Do you know anyone from the XRP Ledger
6 Foundation?

7 A. No, I do not.

8 Q. Do you know anyone who runs an XRP
9 Ledger validator?

10 A. No. Well, I know institutions that
11 were reported in my report that's run XRP Ledger
12 validators.

13 As for persons, if they're private
14 persons, if you ask me that, or somebody
15 maintaining this node, I don't know these people
16 personally.

17 Q. Outside of the information on
18 validators included in your report, do you know
19 anyone who runs an XRP Ledger validator?

20 A. No.

21 Q. Do you know Peter Adriaens?

22 A. No, I do not.

23 Q. Have you ever heard him speak?

24 A. No.

25 Q. Have you read any of his reports in

1 [REDACTED] - Highly Confidential

2 this case?

3 A. I did.

4 Q. What reports of Peter Adriaens have
5 you read?

6 A. I read the rebuttal to my report. And
7 I read his original report.

8 Q. What other expert reports, if any, in
9 this litigation, have you read?

10 A. I read [REDACTED] rebuttal on agent's
11 report. We can classify it as expert's report,
12 right?

13 Q. Yes.

14 A. And that would be it.

15 Q. You say you read [REDACTED] rebuttal
16 report?

17 A. Yes.

18 Q. Are there any U.S. universities that
19 you have worked closely with, Dr. [REDACTED]

20 A. If you define "closely" for me,
21 closely.

22 Q. Well, what -- what U.S. universities
23 have you worked with in any substantive way?

24 A. Let's put it this way, so -- did I
25 ever co-author a paper with somebody. That's an

1 [REDACTED] - Highly Confidential

2 interesting question, actually.

3 So I know many researchers -- let me
4 put it this way. I know many researchers from
5 conferences from different U.S. universities,
6 including Cornell, UT Austin, Brown University,
7 et cetera.

8 Did me -- did I ever -- this is an
9 interesting question. Did I ever co-author, for
10 example, a paper? I don't know, I would need to
11 check.

12 Q. Fine.

13 Have you ever heard of MIT's Digital
14 Currency Initiative?

15 A. I think I heard.

16 Q. Okay. Have you ever interacted with
17 MIT's Digital Currency Initiative?

18 A. No, I didn't.

19 Q. Have you had any interactions with
20 Neha Narula?

21 A. No. I think we were attending maybe a
22 few workshops or conferences, so I know the
23 name. I believe she might know mine, but we
24 never -- I don't think we even talked. No.

25 Q. Do you know whether Ms. Narula has a

1 [REDACTED] - Highly Confidential

2 good reputation in the scientific community?

3 MR. SYLVESTER: Objection.

4 A. You need to define "a good
5 reputation."

6 Q. Do you -- do you know -- do you know
7 anything about her reputation in the scientific
8 community?

9 You know, is she -- is she well
10 regarded? If you know?

11 A. I don't know.

12 Q. Okay.

13 Have you ever met or spoken with Gary
14 Gensler?

15 A. No, I did not.

16 Q. Dr. [REDACTED] do you know what this
17 lawsuit is about?

18 A. I could state it in my words, and then
19 you tell me if I know or don't know. Can I --

20 Q. Go ahead.

21 A. So, what I believe is that SEC is
22 complaining that -- maybe the answer is I don't
23 know. But since I started talking, then I
24 should just finish. But --

25 MR. SYLVESTER: Only say what you

1 [REDACTED] - Highly Confidential

2 know.

3 THE WITNESS: Yes, so what I know.

4 A. So the SE-- the Ripple and the
5 defendants were selling certain products,
6 including, perhaps, the XRP token, as
7 unregistered securities.

8 Q. Do you know what, if any, allegations
9 the SEC has made in this case relating to
10 decentralization?

11 A. I don't -- I don't know.

12 Q. Okay.

13 A. No.

14 Q. Have you read any of the court filings
15 in this case?

16 A. I read the complaint.

17 Q. Okay. When did you review the
18 complaint?

19 A. Very early in the process, so we would
20 be talking again June this year.

21 Q. Why is that not listed in your report
22 as materials that you considered in the case?

23 A. It didn't influence my expert opinion.

24 Q. Do you understand that you were
25 required in this case to identify all materials

1 [REDACTED] - Highly Confidential

2 that you considered, whether or not you
3 ultimately relied on them?

4 A. What does it mean to consider? If I
5 just read them?

6 Q. Yes.

7 MR. SYLVESTER: Objection.

8 A. I was -- so I was -- if this is
9 correct, what you're saying, I was not aware of
10 this. And what I listed is what impacted my
11 expert opinion --

12 Q. So you --

13 A. -- which this complaint did not.

14 Q. I'm sorry, did you finish your answer?

15 A. Which this complaint did not. Yes.

16 Q. So your report only listed materials
17 that you relied on, not that you considered?

18 MR. SYLVESTER: Objection. Misstates
19 his testimony.

20 A. Again, can you please define
21 "considered" for me.

22 Q. Well, I would -- I would -- that is
23 actually a term -- that's a term that is
24 required of all experts. The rule says to --
25 you have to identify materials you considered.

1 [REDACTED] - Highly Confidential

2 For purposes of today, I'll ask it
3 this way. Are there materials that you read,
4 and thought about, and looked through, in --
5 during your work on this case, that you did not
6 cite in your report?

7 A. There are many scientific papers
8 that -- for example, that I didn't cite in my
9 report. Because, for certain concepts, they are
10 very well accepted. So there would be hundreds
11 of papers that refer to this concept, and I
12 didn't make each and every -- for example, if I
13 talk about resilience of distributed and
14 decentralized algorithms, I know literally
15 hundreds of papers, which, you know, they were
16 in my head as someone with 18 years' experience
17 on this topic. Which you can call I considered.
18 Which are not referenced there.

19 But this is like, you know.

20 Q. Yeah.

21 A. Can I reference all the papers that --
22 on the topic that I know about?

23 Would it be useful?

24 Q. Well, your report ultimately lists
25 22 references.

1 [REDACTED] - Highly Confidential

2 How many scientific papers beyond the
3 22 did you look at during the timeframe from
4 June 2021 through the -- you know, through
5 October 4, 2021, when you -- when you issued
6 your report in this case?

7 MR. SYLVESTER: Objection. Limited
8 only to his preparation of the report.
9 Correct?

10 You asked how many papers he looked at
11 in that timeframe. I just want to limit
12 the question to preparing the report.

13 MS. ZORNBERG: That's fine.

14 A. So, it depends again on the definition
15 of "consideration." So, if I'm writing my
16 report, I'm relying on 18 years of experience.

17 So, even if I didn't read the paper in
18 the timeframe you're referring to, I might be
19 considering it because it's part of my
20 understanding of the topic. So that's where the
21 definition of "considering" versus "read" is
22 unclear to me.

23 How many papers? So there were more
24 papers that I read than those that I cite. But
25 I give -- so, yeah. So there -- there are more

1 [REDACTED] - Highly Confidential

2 papers. How many more, I cannot say precisely.

3 Q. So you read more papers in your work
4 on this case than just the ones you cite in your
5 report --

6 MR. SYLVESTER: Objection.

7 Q. -- correct?

8 A. So I -- in the timeframe between --
9 that you're referring to, I read more papers
10 that relate to this topic that -- you know, than
11 what I cite in my report. Yes.

12 Q. Outside of attorneys with the SEC,
13 with whom have you discussed your work on this
14 case?

15 A. With no one. I think my contract
16 allows me to mention the case to my wife, which
17 I did.

18 No one else.

19 Q. Well, you talked about it with [REDACTED]
20 [REDACTED] correct?

21 A. Sorry. Can you -- okay, can you
22 repeat the question --

23 Q. Yeah. Other than SEC --

24 A. -- because I didn't --

25 Q. Other than SEC attorneys, I asked --

1 [REDACTED] - Highly Confidential

2 A. Other than SEC attorneys, yes.

3 Q. -- who -- with whom did you discuss
4 your work on this case.

5 A. Okay. Very good.

6 Q. You said your wife.

7 A. Very good, very good. So with the
8 [REDACTED] -- with the members of the [REDACTED]

9 Q. Did you discuss your work on this case
10 with anyone at [REDACTED]?

11 A. No, I did not.

12 Q. Did you discuss your work on this case
13 with [REDACTED]?

14 A. No, I did not.

15 Q. What did you do to prepare for today's
16 deposition?

17 A. I read Adriaens' rebuttal,
18 Professor Adriaens' rebuttal. I tried to
19 prepare for, essentially, dismissing the points
20 that he makes in his rebuttal.

21 Q. What -- and can you describe what that
22 means? What did you to do to prepare to dismiss
23 points in Professor Adriaens' rebuttal?

24 A. Yes. So Professor Adriaens' rebuttal
25 states, for example, if he cites a paper, he

1 [REDACTED] - Highly Confidential

2 would take certain sentence out of the context.

3 For example -- can I gave an example? May I

4 give an example.

5 Q. Go ahead.

6 A. So I base my basic definition of

7 decentralized systems on the paper by Troncoso

8 and three other authors from 2017. So this is

9 the paper that systemizes 15 years of research

10 in decentralization, and comes up with a

11 definition of decentralized systems.

12 At that paper, so example, what

13 Adriaens did, is that -- there is a motivation

14 in 2017 paper which says it is not well

15 understood how decentralization is defined. But

16 that's the motivation of that paper.

17 And then it continues, it actually

18 says, This is the motivation of our work; hence,

19 we systemized -- systematized 15 years of

20 research and then we give this definition.

21 So Adriaens would take the definition,

22 you know -- definition. Take the sentence.

23 There is no definition. Even Troncoso admits

24 that there is no definition, no -- that's the

25 motivation of their work, and they actually

1 [REDACTED] - Highly Confidential

2 propose the definition.

3 So things like that. And then you go,
4 point by point, and -- yeah.

5 Q. Okay. Who did you meet with from the
6 SEC in preparing for the deposition? Just
7 names, not communications.

8 A. Yes. I met Mark Sylvester.

9 Q. And did you review any documents in
10 preparing for today's deposition that were not
11 cited in your own report of October 2021?

12 A. No, I did not. My report itself was
13 cited in my report. I reviewed my report.

14 Q. Okay. Let's turn to another subject.
15 What digital assets, if any, do you
16 yourself currently own or have you owned in the
17 past?

18 A. [REDACTED] I have owned in the
19 past other -- other digital assets.

20 Q. Okay. So -- so today, sitting here
21 today, the only digital asset you own is

22 [REDACTED]

23 A. Yes. I have interest in [REDACTED] as
24 well, since part of my compensation is in

25 [REDACTED]

1 [REDACTED] - Highly Confidential

2 Q. How much [REDACTED] do you currently own?

3 A. [REDACTED]

4 Q. [REDACTED]

5 A. Yes.

6 With my wife. So it's not my personal
7 owning, so it's like a -- you know, I'm married
8 and things --

9 Q. How did you acquire that [REDACTED]

10 A. All [REDACTED] were acquired by
11 purchasing from my -- so, purchasing on the --
12 today registereds exchanges, so mostly from
13 [REDACTED] so I would take my salary by coins
14 from [REDACTED]

15 Q. When did you first purchase [REDACTED]

16 A. 2017.

17 Q. What's the current value of your
18 [REDACTED] holdings?

19 A. [REDACTED]

20 Q. Why did you start purchasing [REDACTED]
21 in 2017?

22 A. That's an interesting question. So, I
23 would say working in this space -- and this is
24 the blockchain space, et cetera -- so I was
25 starting slowly by experimenting. It's more

1 [REDACTED] - Highly Confidential

2 like do we have skin in the game about the whole
3 space that you are working on. This was the
4 first motivation.

5 And then I invested a bit more when my
6 understanding of [REDACTED] changed and what it
7 actually could do.

8 Q. And when was that?

9 A. So that understanding was -- changing
10 in the understanding was in 2020.

11 In the meantime I also -- so we also
12 invested. [REDACTED]

[REDACTED] So
14 we bought in the -- between 2017 and 2020, but
15 my understanding of [REDACTED] the way -- so not
16 from technical side, it changed in 2020.

17 Q. Did you invest substantially more
18 money in [REDACTED] starting in 2020?

19 A. In 2020 substantially more -- I would
20 say more, yes.

21 Q. Have your ever acquired [REDACTED] by
22 mining?

23 A. No.

24 Q. Have you ever been compensated in
25 [REDACTED]

1 [REDACTED] - Highly Confidential

2 A. No, I did not.

3 Q. Where do you store your [REDACTED]

4 A. [REDACTED]
[REDACTED]

6 Q. Have you ever -- have you ever sold

7 [REDACTED]

8 A. I did.

9 Q. When?

10 A. I did several times. You can say I
11 sold when I -- if I buy a different token, so
12 you sell [REDACTED] to buy that token. So this was
13 in 2017. And my last sale of [REDACTED] was in
14 early 2021.

15 But not for -- so basically for other
16 tokens, at that point I called it a day, and
17 soon after that I moved my holdings back to
18 [REDACTED] with -- [REDACTED].

[REDACTED] Q. When you sold [REDACTED] in 2017, did you
20 sell at a profit?

21 A. I sold it to buy other coins. So if
22 you measure profit in U.S. dollars and -- so --
23 or U.S. dollars or any other fiat currency, then
24 the answer is no because I never did it.

25 Q. Okay. What -- and what coins did you

1 [REDACTED] - Highly Confidential

2 use [REDACTED] to buy in 2017?

3 A. So, I was buying directly [REDACTED] -- so
4 for fiat money, I was buying [REDACTED]
5 at 2000-- in 2017. And probably I bought some
6 minor coins.

7 So I think there was [REDACTED] as a
8 project that's working on data storage. Some
9 other coins I cannot -- you know, I don't have
10 an exact recollection, but these were minor --
11 these were minor amounts.

12 So nothing --

13 Q. Okay.

14 A. -- nothing substantially.

15 Q. So just so we have a clear -- just to
16 clarify, other than [REDACTED] what other digital
17 assets or tokens have you purchased?

18 A. I purchased [REDACTED] and I purchased
19 [REDACTED] on very small amounts at some point.
20 Very early in 2017.

21 And few others. Maybe [REDACTED] I
22 recently purchased [REDACTED] because my son asked me
23 to buy him some [REDACTED] I guess after [REDACTED]
[REDACTED]

25 THE COURT REPORTER: After what?

1 [REDACTED] - Highly Confidential

2 THE WITNESS: [REDACTED]

3 or something like that. When [REDACTED] became
4 popular --

5 MS. ZORNBERG: Did you get that?

6 [REDACTED]

7 A. My son -- my son wanted me to buy him
8 some [REDACTED] And I think --

9 Q. Okay.

10 A. -- yeah.

11 Q. So other than [REDACTED] [REDACTED] [REDACTED]
12 [REDACTED] and [REDACTED] sitting here today, can you
13 think of other digital assets or tokens you've
14 purchased?

15 A. There could be others, minors, for
16 very min-- for like smaller fraction. I don't
17 remember exactly which one.

18 I would definitely not say that the --
19 that the list ends there but honestly not
20 because I'm trying to withhold, because I don't
21 remember.

22 Q. Okay. Have you ever --

23 A. At some point -- at some points for --
24 what I know, what I can recall, I invested in
25 the ICO of [REDACTED]

1 [REDACTED] - Highly Confidential

2 Q. [REDACTED]

3 A. Yes. And so basically, I think -- I
4 remember I sent half a [REDACTED] to [REDACTED] ICO and
5 recovered less than that. So no profits, even a
6 loss in [REDACTED] which is typical when you do
7 these things, yeah.

8 Q. Would you say that among all digital
9 assets, you've purchased more [REDACTED] than
10 anything else?

11 A. We can say that. I probably -- at the
12 beginning, there was -- yeah, more [REDACTED] than
13 [REDACTED] for sure at the beginning. I don't hold
14 any [REDACTED] today.

15 Q. You hold no [REDACTED] now?

16 A. No.

17 Q. Okay. Let's just first finish up on
18 [REDACTED] Then I'll turn to [REDACTED]

19 Have you ever used [REDACTED] to purchase
20 a product?

21 A. No, I did not.

22 Q. Have you ever used [REDACTED] to purchase
23 a service?

24 A. No, I did not.

25 Q. So, can you just describe how much

1 [REDACTED] - Highly Confidential

2 [REDACTED] you -- you've owned at any point and, you
3 know, when you purchased and when you sold?

4 A. I don't remember exactly. I think at
5 some point I had like 100 [REDACTED]

6 But I'm not sure. So everything --
7 that all is conflated now to my [REDACTED]
8 holdings. So...

9 Q. Why did you -- did -- was it your
10 testimony that you transferred your holdings in
11 [REDACTED] to purchase [REDACTED]

12 A. At some point, yes.

13 Q. When was this?

14 A. Last time, end of 2020, beginning of
15 2021.

16 Q. Have you ever used [REDACTED] to purchase a
17 product?

18 A. No, I did not.

19 Q. Have you ever purchased XRP?

20 A. No, I did not.

21 Q. Have you ever held XRP, no?

22 A. I did not.

23 Q. Do you own any NFTs?

24 A. No, I do not.

25 Q. Have you ever used [REDACTED] to purchase a

1 [REDACTED] - Highly Confidential

2 service?

3 A. I did not.

4 Q. Okay. All right.

5 Outside of your work on this case, can
6 you describe your personal or professional use
7 of the bitcoin blockchain.

8 MR. SYLVESTER: Objection.

9 A. Personal or professional use of
10 bitcoin blockchain?

11 I didn't get the question, sorry.

12 Q. Have you ever used the bitcoin
13 blockchain for personal use?

14 MR. SYLVESTER: Objection.

15 A. I still don't understand the question.

16 Like how would you define "personal use"? [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

21 Q. So let me -- let me rephrase the
22 question.

23 [REDACTED]

[REDACTED] how, if at all, have you used the
25 bitcoin blockchain?

1 [REDACTED] - Highly Confidential

2 A. I did not.

3 Q. Have you ever run a bitcoin node?

4 A. I did.

5 Q. You did run a bitcoin node.

6 A. Yes.

7 Q. When did you do that?

8 A. I started two months ago.

9 Q. For what purpose?

10 A. For purpose of further
11 decentralization of the network, to contribute
12 with the small node to further decentralization
13 of the network.

14 Q. Have you ever run a node on a
15 blockchain system other than bitcoin?

16 A. No, I did not.

17 Q. Have you ever run a bitcoin miner?

18 A. No, I did not.

19 Q. So the node that you started to run
20 two months ago can participate in validation but
21 does not mine?

22 A. Yes.

23 Q. Have you ever submitted a bitcoin
24 improvement proposal?

25 A. No, I did not.

1 [REDACTED] - Highly Confidential

2 Q. Have you conducted research projects
3 specifically using the bitcoin network?

4 A. Currently, we are doing a similar
5 project. It's not exclusively using bitcoin
6 network, but it's using the bitcoin network.

7 Q. What project is that?

8 A. This is the project of anchoring the
9 membership of proof of stake, like blockchains,
10 into bitcoin.

11 Proof-of-stake blockchains have an
12 attack surface when they reconfigure membership.
13 This is actually similar to accept the ledger.
14 And when you change the membership, this is the
15 pain point of these protocols.

16 So if you put concisely the membership
17 of the network into the bitcoin blockchain, you
18 get more security out of the whole system
19 together.

20 Q. Is that a project you're doing for
21 [REDACTED]?

22 A. You can say I'm doing it -- I started
23 it in [REDACTED] I continued while I'm working with
24 [REDACTED]. I wouldn't use the word "for."
25 I would say the [REDACTED] knows, of course,

1 [REDACTED] - Highly Confidential

2 and supports that I'm doing this project, and
3 yes, I would put it this way.

4 Q. And just -- would it be fair to say
5 that your -- your project involves using a
6 development on the -- hold on.

7 Say it one more time.

8 A. Yes.

9 Q. Explain how does -- how does the
10 project relate Ethereum to the -- to the bitcoin
11 network?

12 MR. SYLVESTER: Objection.

13 A. Ah, so I didn't say Ethereum.

14 Q. Okay. So tell me --

15 A. I was talking about proof-of-stake
16 family of protocols. And also, Byzantine full
17 tolerance protocols. They -- they are very
18 similar, so proof of stake and Byzantine full
19 tolerance protocols, they are -- they are very
20 close to each other.

21 Their pain point is the -- so if you
22 have a static membership -- static membership
23 meaning membership doesn't change -- then you
24 can run Byzantine Full-Tolerant protocols, and
25 that works. This is like how we understand

1 [REDACTED] - Highly Confidential

2 them, that would work.

3 It would come with a big assumption.
4 It's usually you have a threshold of the number
5 of Byzantine nodes that such a protocol can
6 tolerate. And that's static, that's fixed in
7 time.

8 So if you start modifying the
9 membership, you are starting playing with the --
10 with the -- essentially which nodes.

11 For example, to give you -- give you
12 an example. In proof-of-stake protocols, what's
13 dangerous is that current power of the network
14 is relate to the stake of the validators.

15 And we have a snapshot in time in
16 which, you and me, we have the power in the
17 network, but then, we are transferring this
18 stake to others. But we are keeping the
19 cryptographic keys from this point in time.

20 So basically, once we don't have the
21 stake in the network, we can essentially invent
22 another history that would be valid because we
23 were valid validators at some point, and if we
24 present two alternative histories to the client,
25 the client couldn't tell which one to believe

1 [REDACTED] - Highly Confidential

2 because they're both legitimate.

3 Now, what you -- what the client could
4 say is this one that evolved first, is the right
5 one, but how do you know which one is the first.

6 Q. So how is your project trying to solve
7 for what you've described?

8 A. Great question. Thank you so much.

9 So it would, from time to time, as --
10 for example, this first -- as we are
11 transferring tokens to others.

12 When the system sees that there is a
13 lot of difference between the membership --
14 membership or the stakeholders at certain
15 snapshot of time, and the other, it would go and
16 checkpoint this information of the new members
17 and the new stakeholders to the bitcoin
18 blockchain, which doesn't suffer from this
19 because of the way consensus protocol works in
20 bitcoin. We can just checkpoint this
21 information into bitcoin.

22 And basically, then, in order to mount
23 the attack that I just described, you would need
24 to mount the attack on bitcoin as well, to forge
25 that network, in order for that work on your

1 [REDACTED] - Highly Confidential

2 network.

3 So you're actually gaining more
4 security from the -- in a proof-of-stake
5 blockchain or Byzantine fault-tolerant protocol
6 from the proof-of-work protocol. You're getting
7 the security from there.

8 Q. So your proposal would have
9 proof-of-stake networks rely on bitcoin network
10 for certain aspects of security?

11 A. Yes.

12 Q. Okay. Are you -- is it your view that
13 a BFT protocol works well only if membership is
14 static?

15 MR. SYLVESTER: Objection.

16 A. Depends on the definition of the
17 protocol. So it's much better understood how it
18 works, and the security properties are much more
19 easier to guarantee and prove if the membership
20 is static.

21 Q. So sit -- so sitting here today, are
22 you saying that BFT protocols will only work
23 well if membership is static?

24 A. No.

25 MR. SYLVESTER: Objection. Misstates

1 [REDACTED] - Highly Confidential

2 his testimony.

3 THE WITNESS: Yes.

4 Q. Okay. So you're not --

5 A. I'm not saying that.

6 Q. Okay. Have you ever run an Ethereum
7 node?

8 A. I did not.

9 Q. Have you ever run an Ethereum miner?

10 A. No, I did not.

11 Q. Have you ever proposed changes to the
12 Ethereum consensus protocol?

13 A. I did not.

14 Q. Have you done any research projects --
15 putting aside the proof-of-stake project that
16 you've just described you're currently working
17 on, have you done any research projects
18 specifically relating to Ethereum?

19 A. The predecessor of that project was
20 trying to do the same what I described,
21 checkpointing into bitcoin network, checkpoint
22 into Ethereum proof-of-work network, because so
23 long as you have a proof-of-work protocol, you
24 can do this thing.

25 And we had one protocol, one --

1 [REDACTED] - Highly Confidential
2 basically the predecessor to the work of
3 checkpoint into bitcoin that I'm describing,
4 that we did as a -- while I was still in IBM,
5 actually. We did -- we checkpoint into Ethereum
6 assuming Ethereum runs on proof of work. So
7 it's important which class of protocol
8 checkpoints into which. You cannot
9 checkpoint --

10 Q. Right.

11 A. -- proof of stake into proof of stake
12 that doesn't make sense, but you can checkpoint
13 proof of stake to proof of work.

14 Q. So have all of your checkpoint
15 research projects involved creating an extra
16 checkpoint on a proof-of-work network?

17 A. Yes, they did.

18 Q. Okay. Outside of your work on this
19 case, have you ever used the XRP Ledger?

20 A. I did not.

21 Q. Well, including your work on this
22 case, even during your work on this case, did
23 you use the XRP Ledger?

24 A. No, I did not.

25 Q. Why not?

1 [REDACTED] - Highly Confidential

2 A. I didn't. So while I was analyzing
3 the -- mostly the internals of the consensus
4 protocol, I was inspecting the code, as I
5 mentioned. And I was expecting -- inspecting
6 the papers which were endorsed by Ripple
7 employees.

8 To -- for me to gain the understanding
9 of how the protocol works, I gained it without
10 running the node.

11 Q. Okay. So have you ever run a node on
12 the XRP Ledger?

13 A. No, I did not.

14 Q. Have you ever run a validator on the
15 XRP Ledger?

16 A. No, I did not.

17 Q. Have you ever proposed changes to
18 Ripple D?

19 A. No, I did not.

20 Q. Have you ever conducted research
21 projects relating to the XRP Ledger?

22 A. Apart from the paper that we
23 discussed, if you call that, that would be a
24 yes. Or otherwise, no.

25 Q. And the paper that we discussed,

1 [REDACTED] - Highly Confidential

2 you're referring to the 2017 --

3 A. '17 paper, yes.

4 Q. -- paper.

5 Okay.

6 A. Yes.

7 Q. Have you -- while at [REDACTED] did any of
8 your work projects involve the XRP Ledger?

9 A. No, they did not, apart from -- yeah.

10 Q. Are you aware that the XRP Ledger
11 contains a decentralized exchange?

12 A. I think I heard about something that
13 would go along these lines. I'm very about
14 calling things decentralized, as you may
15 imagine, without looking more deeply into that.

16 Q. So you -- you don't really know?

17 A. If you -- if you tell me, Do I know if
18 it runs on decentralized exchange, I say yes,
19 then I might be admitting that it's
20 decentralized, so this is not what I'm doing.

21 So I heard, I have -- I have
22 understanding that some people run something
23 which they call decentralized exchange on the
24 Ripple -- on the XRP Ledger.

25 Q. Have you ever used it?

1 [REDACTED] - Highly Confidential

2 A. No.

3 Q. Do you know what the Interledger
4 Protocol is?

5 A. Not -- no.

6 Q. Okay.

7 All right. We're going to mark -- or
8 show you what's been premarked, actually --

9 MR. SYLVESTER: Louise, we're at about
10 an hour. Should we take a break before you
11 mark?

12 MS. ZORNBERG: If -- if Dr. [REDACTED]
13 wants to take a break, we can break.
14 Otherwise I want to -- I'd -- I'd push
15 through, but if this a convenient time.

16 THE WITNESS: Yeah, let's -- let's
17 take a break, yeah.

18 MS. ZORNBERG: Ten minutes? How --

19 THE WITNESS: Ten minutes.

20 THE VIDEOGRAPHER: The time is
21 9:24 a.m. We're going off the record.

22 (Recess from 9:24 to 9:39.)

23 THE VIDEOGRAPHER: It is 9:39 a.m. We
24 are back on the record.

25 Q. All right. Dr. [REDACTED] I'm showing

1 [REDACTED] - Highly Confidential

2 you what's been marked as Exhibit [REDACTED] 1.

3 (Expert Report of [REDACTED]
4 Ph.D., was marked [REDACTED] Exhibit 1 for
5 identification, as of this date.)

6 Q. Is this a copy of your expert report
7 in this case?

8 (Witness reviewing document.)

9 A. Yes, it is.

10 Q. Okay. And on page 28, is that your
11 signature?

12 A. Yes, it is.

13 Q. Does this report contain all of the
14 opinions that you're expressing in this case?

15 A. This report contains all the -- yes.

16 Q. I'm asking, because if -- if there are
17 any --

18 A. Yes, if there -- yeah, so what I wrote
19 in my paper, maybe. But my report, if there are
20 any additional -- so provided with all the
21 information I got until that date.

22 If there are new developments, I
23 reserve the right to supplement my report.

24 Q. Well, are there additional opinions
25 that you're offering in this case that are not

1 [REDACTED] - Highly Confidential

2 contained in your report? As you sit here
3 today.

4 A. Yes. If -- as of my -- so in
5 particular, my report is related to a snapshot,
6 as I've explained on the -- on the software.

7 If the software changes, there could
8 be additional opinions.

9 Q. Okay. Sitting here today,
10 Dr. [REDACTED] are you -- are there additional
11 opinions, as you sit here today, that you're
12 offering in this case?

13 A. I know there are other changes, to the
14 software, which might change certain things that
15 I wrote in this report.

16 And they actually happened after the
17 report was submitted.

18 So I know about that. But I'm not --
19 I'm reserving the right. So in some cases, it
20 would take me more time to form this depth of
21 the opinion. So I wouldn't necessarily offer
22 them today. I -- in some cases, I would require
23 more time to, for example, analyze the software
24 changes in depth, to adapt my report to the new
25 reality, right? So you always need to -- when

1 [REDACTED] - Highly Confidential

2 you have already decentralized system, you're
3 actually taking a snapshot in time.

4 Q. What changes in the software for the
5 XRP Ledger have been made since October 4, 2021,
6 that you're referring to?

7 A. To my understanding and what I checked
8 is that there are two validator list sites
9 instead of one. So Ripple 1.7.3, there are --
10 there was one validator list site, which was
11 important for the things I wrote in the paper,
12 in the report. And that was controlled at the
13 URL vl.ripple.com.

14 So there was another one added to the
15 configuration, default configuration file, plus
16 recently there is update that's called
17 Negative UNL. That was in the software since
18 2020, but it was not active. So in a sense, it
19 didn't influence the operation of --

20 Q. Okay.

21 A. -- the software.

22 But it was, to my understanding,
23 activated on 23rd of November, so just recently.

24 Q. All right. Let's take those two for a
25 minute. You said that since your report in this

1 [REDACTED] - Highly Confidential

2 case, you've seen that the -- the rippled code
3 now contains two validator list sites.

4 Correct?

5 A. Yes.

6 Q. Does that change in the rippled code
7 affect any of the opinions you previously
8 expect -- expressed in your report?

9 A. We would not go in -- you would need
10 to go in details to see. There are certain
11 sentences that I say. For example, I'm pretty
12 sure I say at some point that only -- that the
13 only validator list sites listed in the
14 configuration file is Ripple. That's obviously
15 need to be amended.

16 In general and on a high level, does
17 it influence -- because in the report, I'm
18 accepting the Troncoso definition that a system
19 is decentralized if no single authority is fully
20 trusted by all. That change doesn't impact the
21 fact that XRP Ledger, according to that
22 definition, cannot be classified as
23 decentralized. So it doesn't impact the main
24 finding of the report.

25 Q. What -- what opinions in your report

1 [REDACTED] - Highly Confidential

2 have changed based on the change in the software
3 listing to validator lists?

4 MR. SYLVESTER: Objection.

5 A. I would need to spend more time, so
6 basically, I'm offering at that -- at this
7 moment, I'm offering my opinion on the current
8 report. I would need more time to -- in
9 details, so I don't want to tell you certain
10 things now online and then not be sure that
11 these are all the implications. So basically,
12 that -- so if I say it affects Sentence A, I
13 need to just process and be sure that it affects
14 Sentence A; but I also need to be sure that
15 if -- you know, if I don't say it affects
16 Sentence B, that this is actually the case; it
17 may be affecting Sentence B, and I need more
18 time to go through that.

19 Q. You're not prepared to do that today?

20 A. I'm not prepared to do that today in
21 details. I can discuss certain high-level
22 things. Yes.

23 Q. At a high level --

24 A. Yes.

25 Q. -- how do you think it could affect

1 [REDACTED] - Highly Confidential

2 your opinions in this case that the rippled
3 software lists two validator sites?

4 A. It will -- just let me refer to my
5 report.

6 (Witness reviewing document.)

7 A. For example, I see one thing that is
8 not necessarily so. I see one item that would
9 not need to be done by Ripple anymore.

10 Q. What are you referring to? What page?

11 A. Page 25, item 1. But this is an
12 example. I would -- you know, before we go into
13 details, I would just give an example. So I
14 gave you an example of my opinion that doesn't
15 change, which is the qualification of the
16 XRP Ledger on the Troncoso definition it would
17 remain centralized. I'm giving you an example
18 of what changes.

19 Q. Okay. And --

20 A. And then for exhaustiveness of this,
21 we would need -- I would need more time to make
22 sure, you know, that this is one that I notice,
23 aha, this would change. So we can discuss that.

24 Page 25 -- sorry.

25 Page 25 at the top of the page.

1 [REDACTED] - Highly Confidential

2 Q. Okay.

3 A. So --

4 Q. So let's just -- let's just be clear
5 for the record. Page 25 at the top of the page
6 contains your answer to the question, E2, quote,
7 To what extent have Ripple's efforts been needed
8 to support the proper functioning of the
9 XRP Ledger, closed quote?

10 Right?

11 A. Yes.

12 Q. Okay. So you're saying that the
13 change, you've noticed recently of there being
14 two validator lists in the rippled code, could
15 impact your answer to that question.

16 MR. SYLVESTER: Objection.

17 A. Yes. So it could impact my answer to
18 that question, assuming that the protocol
19 changed. So in my -- for the specifics of my
20 report, which are discussed and I'm getting --
21 if I fix my opinion to my report, my report
22 sticks -- my opinion with rippled 1.7.3. So it
23 wouldn't change this. If you say, Would I
24 change my opinion? And this refers to 1.7.3,
25 the answer is, no, it wouldn't change.

1 [REDACTED] - Highly Confidential

2 If new elements are presented as of
3 October 4, and this happened after October 4, if
4 I would be in a hypothetical case where I would
5 be assuming the new version of the code and
6 writing this report as of Ripple 1.8.1, this
7 would change.

8 MS. ZORNBERG: Okay. Let's show
9 Exhibit 13.

10 Q. And while we're getting that exhibit,
11 I would like to direct your attention to the
12 bottom of page 20 of your report.

13 In the last -- in the last paragraph,
14 of your report, you reference the validators
15 example text file. Correct?

16 A. Sorry. Can you repeat? I was --

17 Q. Yeah. Page 20 of your report.

18 A. Yes.

19 Q. The very -- it's the very last
20 sentence on the page that ends on the top of
21 page 21. In that part of your report, you
22 reference the validator example .text file.
23 Correct?

24 A. Yes.

25 Q. Okay. So please take a look at what's

1 [REDACTED] - Highly Confidential

2 been marked as Exhibit [REDACTED] 13.

3 (Document was marked [REDACTED] Exhibit 13 for
4 identification, as of this date.)

5 A. Yes.

6 Q. Do you recognize this document?

7 And I'm basically asking, is this the
8 document -- is this the -- what you've cited, at
9 the very last line of your report, on page 20?
10 The cite.

11 A. It is not. So --

12 Q. Why is it not?

13 A. So just a second.

14 (Witness reviewing document.)

15 Q. Dr. [REDACTED] doesn't the -- the actual
16 citation at the last line of your report,
17 page 20, match exactly to --

18 A. Yes.

19 Q. -- the GitHub site at the top of
20 Exhibit 13?

21 A. It does. I see where the error is.
22 Okay.

23 Q. Okay. What is the error that you're
24 seeing?

25 A. The error is that this is the cite --

1 [REDACTED] - Highly Confidential

2 so the link that I put, so I'm always referring
3 to the code that was in the release, 1.7.3.

4 And this was on the develop branch.

5 So basically, the link that I'm giving, by
6 error, is referring to the development branch,
7 which is not in the release branch. So you can
8 see by the URL mentioned the develop.

9 Q. Okay.

10 A. So the development, yes, in the
11 development branch, the second validator list
12 site was mentioned for a long time, but this
13 doesn't affect the release.

14 Q. Okay. So you're saying there's an
15 error in your report in including that citation?

16 MR. SYLVESTER: Objection.

17 A. Yes. So there is -- what I meant here
18 is to refer to the release branch. And I
19 think -- so not I think.

20 I basically say that in page 19,
21 Item 3, I'm referring to rippled software on its
22 release branch.

23 And then I'm probably by omission
24 giving the -- the development branch, which you
25 can see the URL denoted as develop.

1 [REDACTED] - Highly Confidential

2 Q. If you turn your attention to lines 57
3 and 58 --

4 A. Yes.

5 Q. -- of Exhibit 13.

6 Would you agree that those lines of
7 code identify one validator list for
8 vl.ripple.com and one for vl.xrplf.org?

9 A. They do.

10 Q. What do you understand that to mean?

11 A. So this is -- basically, this was in
12 the development branch but not in the release of
13 1.7.3.

14 This was propagated to the release.
15 This is the change that we discussed after my
16 report which propagated to the release branch of
17 1.8.1, if I'm correct. This means that a server
18 which periodically refreshes the dUNL, instead
19 of going only to vl.ripple.com and no other site
20 as a release 1.7.3, would now first go to the
21 vl.ripple.com. And then if this doesn't work,
22 it would go to xrplf.org.

23 Q. How long was -- did this commit exist
24 in the code?

25 MR. SYLVESTER: Objection.

1 [REDACTED] - Highly Confidential

2 A. I'm not sure. If we look at the
3 document that you gave me, it says, Latest
4 commit on May 10. Need to observe that this is
5 the commit to the development branch.

6 Q. Okay. And you -- you considered this
7 before you wrote your report, correct?

8 A. I saw this before I -- before I wrote
9 my report.

10 Q. Okay.

11 A. I was focusing on the release branch
12 as I pointed out on page 19, Item 3.

13 Q. All right. Let me just show you
14 briefly, Exhibit 13A.

15 And that would be Exhibit [REDACTED] 13A.

16 (History Page was marked [REDACTED] Exhibit
17 13A for identification, as of this date.)

18 Q. I'll represent to you that Exhibit 13A
19 is what -- is the page you get if you click on
20 the link in Exhibit 13, that says, History.

21 So this is the page that shows up as
22 history.

23 Did you ever review Exhibit 13A in
24 your work on this case?

25 A. This is -- so as you presented it

1 [REDACTED] - Highly Confidential

2 here, I did not have this list. This is mostly
3 related to the development branch again.

4 Q. Okay.

5 A. And I focused my findings on the
6 rippled release Version 1.7.3, as pointed out on
7 page 19, item 3.

8 Q. And the history, in Exhibit 13A, do
9 you agree it shows that a commit was made on
10 July 27, 2021, to add the XRP Ledger Foundation
11 to the validator list sites?

12 A. This is the commit, yes, that affected
13 the development branch --

14 Q. Did you --

15 A. -- which means at that point -- which
16 means at that point if somebody downloads the
17 releases code, it gets -- it is not affected by
18 this change.

19 Q. Did you consider this commit at any
20 time before July 27, 2021?

21 A. If you asked me did I saw that the
22 development branch has two validator sites, it
23 does. I did.

24 I took a snapshot of the release
25 talking about with one validator list site.

1 [REDACTED] - Highly Confidential

2 Q. So --

3 A. Yes.

4 Q. So Dr. [REDACTED] if you were aware of
5 this code change in development before you wrote
6 your report in this case, why did you not --
7 what -- did you consider it -- did you consider
8 it in writing your report in this case?

9 MR. SYLVESTER: Objection.

10 A. I -- well, if -- what I read, I
11 considered, you can say I had it in mind. So
12 you can say I, you know, considered it in the
13 sense of consideration that we discussed before.

14 When you talk about decentralization
15 of a certain blockchain, you need to fix the
16 code.

17 This is a development branch. Things
18 can come, go, and back from the development
19 branch.

20 So for that purpose I'm focusing on
21 the release branch. Now we can -- I mean, so
22 this propagating to if I were writing the report
23 now, I would need to consider this change and
24 include it in my report because now, only now,
25 after I submitted my report, it's in the

1 [REDACTED] - Highly Confidential

2 release.

3 Q. And what would happen if a validator
4 used this configuration in Exhibit 13, for its
5 Unique Node List?

6 A. I think we discussed it. So if this
7 means that it go would to vl.ripple.com and
8 fetch the -- try to fetch the UNL from there, if
9 this doesn't work, it would go to the
10 vl.xrplf.org and try to fetch the UNL from
11 there.

12 Q. Would the validator recognize the
13 nodes on both lists as trusted?

14 A. It would -- so from the perspective of
15 the node, it would continue its operation,
16 regardless of where it fetches the UNL from.

17 Q. So is that yes?

18 A. Can you repeat the question?

19 Q. Yeah. Would a validator using the
20 configuration code in Exhibit 13 recognize the
21 nodes on both UNL lists as trusted?

22 A. I wouldn't say so trusted -- it would
23 continue operation of the protocol, regardless
24 of the place it fetched the UNL from.

25 Whether they are trusted or not, I

1 [REDACTED] - Highly Confidential

2 mean, if the -- so if the node would trust the
3 UNLs that it gets from the validator list sites,
4 the answer would be yes.

5 Q. Can a server run the development
6 branch?

7 A. You can install the development
8 branch, sure, run it in production yes, you can.

9 Q. Okay. And is it your understanding
10 that the UNL at Ripple and the XRPL Foundation
11 UNLs -- hold on. Let me rephrase.

12 Do you know one way or another if the
13 UNLs at the Ripple's published UNL and the
14 XRPL Foundation's UNL are identical?

15 A. I do not know for sure.

16 Q. Okay. All right.

17 Were there drafts of your final
18 report, prior to this final version in
19 Exhibit 1?

20 A. There were.

21 Q. Did you show those drafts to anyone?

22 A. I showed them to [REDACTED]

23 Q. Do you know who [REDACTED] showed them
24 to?

25 A. I suspect that they showed them to the

1 [REDACTED] - Highly Confidential

2 SEC.

3 Q. Who at [REDACTED] reviewed your draft?

4 A. [REDACTED] [REDACTED] mostly. At
5 some point [REDACTED] I don't remember last name.
6 I'm not sure [REDACTED] reviewed it, but I don't think
7 I got any comments from [REDACTED]

8 Q. And did [REDACTED] and the others at [REDACTED]
9 aside from [REDACTED], provide comments?

10 A. Sorry. Can you repeat? Did [REDACTED]

11 Q. Did anyone at [REDACTED] or the SEC
12 provide comments on your draft report?

13 A. So --

14 MR. SYLVESTER: Objection. With
15 respect to the SEC, any SEC comments, I
16 just instruct you not to get into the
17 substance of any communications between any
18 SEC attorney and yourself.

19 A. So SEC and [REDACTED] yeah, they
20 provided comments on my draft, yes.

21 Q. Okay. You identify two changes, in
22 the software, rippled, since your report was
23 issued, that might change your opinions.

24 The first we've just talked about, the
25 two validator lists. You also mentioned a

1 [REDACTED] - Highly Confidential

2 Negative UNL update.

3 A. Yes.

4 Q. What is that?

5 A. To my understanding, which is -- so
6 that's a substantial protocol change which
7 doesn't affect dUNLs. So when you reason about
8 decentralization of the system of the dUNL, this
9 Negative UNL doesn't really impact that aspect
10 of centralization.

11 Now, Negative UNL, to my
12 understanding, but I would definitely need time
13 to dive into more details of that, to my
14 mid-level understanding, is that what it does is
15 it takes this dUNL and doesn't treat it as a
16 fixed line, assuming that you get always the
17 same UNL from the validator list site.

18 Now, this not a static configuration,
19 but this can change basically -- now, I'm
20 getting into the territory where I need more
21 time to inspect, but based on how nodes behave
22 on the network, you can exclude them from the
23 UNL.

24 Q. How might that change in the
25 rippled code affect the opinions you've given in

1 [REDACTED] - Highly Confidential

2 this case?

3 A. For that I would need more time to
4 opine.

5 Q. Sitting here today, you're not
6 prepared to say one way or another if it affects
7 your opinions --

8 A. I can say it does not impact the main.
9 So it doesn't make XRP Ledger suddenly pass the
10 Troncoso definition because it doesn't have --
11 so neither of the two changes that I can say
12 make XRP Ledger pass the Troncoso definition
13 because we still need to trust a single
14 authority. We can go into details why.

15 There might be other parts of the
16 paper. Notably I would need to understand, you
17 know, does it impact my Appendix B attack or
18 some other point in the paper? But for that I
19 would not offer any other opinion before I have
20 time to opine on that.

21 It's a very -- it's a substantial
22 change. It's an interesting one. It's an
23 interesting one. But -- and I would actually
24 like to have more time to look at it, but I
25 didn't.

1 [REDACTED] - Highly Confidential

2 Q. Has the SEC given you the
3 assignment -- any assignments beyond the
4 issuance of the report you've already done in
5 this case?

6 A. No.

7 Q. So you've not been asked -- sitting
8 here today you've not been asked by the SEC to
9 offer a supplemental opinion?

10 A. No.

11 Q. So why don't you tell us, what is your
12 view as to -- going back to the two validator
13 list sites that you've acknowledged are now in
14 the rippled code, why does that not change your
15 opinion that -- that there is still a single
16 trusted -- hold on. Let me rephrase.

17 You've said that the two validator
18 lists sites do not affect your opinion on how
19 the Troncoso definition applies to the
20 XRP Ledger. Please explain why.

21 A. Assume vl.ripple.com is the first
22 validator list site. Let's assume that it
23 doesn't disappear; it continues publishing the
24 list. It just serves -- the different list is
25 the attack that I'm describing for the untrusted

1 [REDACTED] - Highly Confidential

2 validator list site. It just serves a different
3 dUNL -- continues serving different dUNLs to
4 different nodes.

5 It can break safety line as properties
6 of the system, regardless of the adding of the
7 second one. You can add third and fourth and
8 fifth, and it doesn't really matter.

9 In the way they are added, like one by
10 one, one after the other.

11 Q. So your view is that it doesn't matter
12 how many UNL validator lists are referenced in
13 the rippled code, no matter what? Even if there
14 are a hundred, it's still a centralized system?

15 A. Why? Because if you default to first,
16 as the software goes and defaults first to
17 first, and that one is working, it can serve
18 different UNL to different nodes, hence by
19 actually invalidating, so making the UNL overlap
20 nonexisting.

21 And as we know from the analysis which
22 I confirmed through my inspection of the code,
23 this overlap is required. And you would need to
24 trust the first validator site on the list, that
25 it doesn't serve a different UNL.

1 [REDACTED] - Highly Confidential

2 And then if that one doesn't work,
3 you're defaulting to the second one. You need
4 to trust that one. So let's assume
5 vl.ripple.com doesn't exist anymore. Everybody
6 goes to vl.xrplf.org and now everybody needs to
7 trust vl.xrplf.org that it's not -- that it
8 doesn't serve different UNLs for different
9 people.

10 So somehow, what this contributes to
11 the protocol, is it improves in some sense
12 availability if validators list sites are not
13 trying to cheat others. It would help you that.

14 But it still assumes that validator
15 list sites do not cheat to validator nodes.

16 Q. What is the basis for your statement,
17 that there's still a default validator list when
18 there's more than one listed in the code?

19 A. So because the software is defaulting
20 to the first one; and then if it doesn't work,
21 it goes -- it goes to the second one.

22 Q. What is that based on?

23 A. Based on my analysis of the protocol.

24 Q. Is it your understanding that
25 validators will only use the first working

1 [REDACTED] - Highly Confidential

2 listed UNL in the code?

3 A. While it works. Yes. While it
4 replies.

5 Q. So it's your understanding that if
6 there are two that are listed, that validators
7 will only use the first one and never reach the
8 second one as long as the first is working?

9 A. This is my understanding of software,
10 yes.

11 Q. Are you -- are you a hundred percent
12 sure of that?

13 MR. SYLVESTER: Objection.

14 A. Yes.

15 Q. Okay.

16 A. Let's -- yeah, let's say, because this
17 was not the -- this was not the part of the
18 software I was -- analyzed when I did, I would
19 need more time to give you 100 percent answer.
20 And I'm pretty sure this is the case.

21 Q. Okay. So your testimony is that
22 you're pretty sure, but you're not a hundred
23 percent sure.

24 A. I would need more time because this is
25 a change that affected my report.

1 [REDACTED] - Highly Confidential

2 Q. Okay.

3 A. Under this understanding, this is
4 what's happening.

5 Q. Okay.

6 A. Let me make sure that this is -- so
7 with additional time, I can make sure that this
8 is -- actually you understand.

9 Q. To be clear, I'm not requesting that
10 you do anything.

11 A. Yes.

12 Q. Although I am requesting that you turn
13 to the curriculum vitae that is contained in
14 your report.

15 And my question is, when did you most
16 recently review your curriculum vitae?

17 A. I think I reviewed it before
18 submitting it to this -- before sending the
19 report. So late September, early October.

20 Q. Okay.

21 MS. ZORNBERG: Can everybody on Webex
22 please go on mute.

23 Q. Okay. So you last reviewed the
24 curriculum vitae in September?

25 A. Yes.

1 [REDACTED] - Highly Confidential

2 Q. Okay. Is there anything that
3 should -- that you would want that's new since
4 October 4, 2021, that you would want to add?

5 (Witness reviewing document.)

6 A. So the first paper on the publication
7 list on page 6 of the appendix that appears, in
8 the meantime -- yeah. I don't think there are
9 any substantial change.

10 Q. Okay. So I just want to briefly
11 review with you your educational background.

12 A. Yes.

13 Q. You have a degree in electrical
14 engineering from the [REDACTED] in
15 2021. Yes?

16 A. Yes.

17 Q. And you got your Ph.D. in distributed
18 systems in 2008?

19 A. Yes.

20 Q. And that was from the [REDACTED]
[REDACTED]

[REDACTED]? Right?

23 A. [REDACTED]
[REDACTED] is the school at [REDACTED] [REDACTED] is the
25 university, [REDACTED]

1 [REDACTED] - Highly Confidential

2 [REDACTED]

3 Q. Thank you for that clarification.

4 How much of your educational training
5 was in coding?

6 MR. SYLVESTER: Objection.

7 A. How would I -- what do you mean?

8 Q. Well, I'm trying to understand if
9 you -- what is your coding capability?

10 MR. SYLVESTER: Objection.

11 A. How do you measure coding capability?

12 Q. Do you consider yourself a coder?

13 A. I consider myself a coder, yes.

14 Q. Yes. Okay. Do you consider yourself
15 an expert in computer coding?

16 A. I -- we would need to define "expert
17 in computer coding." There are certainly other
18 people who can code better than me. Yes.

19 Q. For the development -- have you worked
20 on development projects where you yourself are
21 the coder of those projects?

22 A. Yes, I did.

23 Q. Okay.

24 What language do you code in?

25 A. The last contributions were in Go.

1 [REDACTED] - Highly Confidential

2 Go. Go on. Go. Go. Go.

3 Q. Can you spell that?

4 A. G-O.

5 Q. G-O. Okay.

6 A. Yes.

7 Q. Thank you.

8 Besides your undergraduate degree in
9 electrical engineering and your Ph.D. in
10 distributed systems, have you received any other
11 formal education training?

12 A. Formal as in a degree? No.

13 I mean, I went to high school. You're
14 not probably saying that. Yes.

15 I went to high school and elementary
16 school, yes.

17 Q. Yes. Okay.

18 Do you hold a degree in economics?

19 A. I do not.

20 Q. Have you done any formal academic
21 training in economics?

22 A. I did not.

23 Q. Do you have an MBA or an equivalent
24 degree in business?

25 A. I have a micro MBA, which doesn't

1 [REDACTED] - Highly Confidential

2 qualify as MBA. I have a micro MBA from a
3 course that I took while in [REDACTED]

4 Is it mentioned?

5 Q. Is that -- is that reflected in your
6 CV?

7 A. No. It's a one-week course. You can
8 disregard it if you want.

9 Q. Okay.

10 A. I was elected the best CEO of that
11 week, but -- yeah.

12 Q. Okay. So it was a one-week training
13 class on business.

14 A. You can put it that way.

15 Q. Beyond the one-week training class in
16 business at [REDACTED] have you received any formal
17 training in business or business management?

18 A. I did not.

19 Q. Have you received any degrees or
20 formal academic training in the areas of
21 innovation and entrepreneurship?

22 A. Can you repeat it again. Sorry.

23 Q. Do you hold a degree in innovation?

24 A. No. I mean, innovation as in --
25 what's a degree in innovation.

1 [REDACTED] - Highly Confidential

2 Q. You know, I'm not --

3 A. I mean, by getting a Ph.D. and doctor,
4 I innovated something, so I got a degree in
5 innovation. But I -- it's not called that way.

6 Q. Okay. Is it -- is it fair to say that
7 to the extent there are universities that offer
8 degrees in entrepreneurship studies or
9 innovation studies styled in that way, you've
10 not received degrees in those areas?

11 A. There is a degree in innovation and
12 entrepreneurship. I did not.

13 Q. How about environmental science? Have
14 you received any degree in environmental
15 science?

16 A. I did not.

17 Q. Have you taken any academic coursework
18 on environmental science?

19 A. I did not.

20 Q. Do you consider yourself an expert in
21 the field of environmental science?

22 A. I did not.

23 Q. How about in the field of business?
24 Do you consider yourself an expert in business
25 management?

1 [REDACTED] - Highly Confidential

2 A. I do not.

3 Q. What is the distributed blockchain
4 system?

5 A. Distributed blockchain system is a
6 different definition. It's a distributed
7 system, meaning there's several computers that
8 are contributing that are working towards a
9 common goal, roughly speaking. The famous
10 definition of the distributed systems, by
11 Tanenbaum that I cite in my report says that
12 distributed systems appear to the end users as a
13 single coherent system. "Coherent" is a bit
14 vague there. It depends on the specification of
15 the system.

16 But systems function as -- as one,
17 regardless of the fact that it's executed on
18 different machines, on distributed machines.

19 So that would be a distributed system.

20 Now, the blockchain system is
21 typically a distributed system in which there is
22 a data structure, which reminds of a blockchain.
23 So there is a chain of blocks. There are --
24 there is certain data contained in the block.
25 And the blocks are linked, usually

1 [REDACTED] - Highly Confidential

2 cryptographically to each other.

3 Q. Do you consider bitcoin, Ethereum, and
4 the XRP Ledger all to be distributed blockchain
5 systems?

6 A. I do.

7 Q. Okay. And do you consider the terms
8 "blockchain system" and "distributed ledger
9 system" to be interchangeable?

10 A. We can say that on a high level, yes.
11 It requires definitions of both of the terms.
12 But people, when they say "blockchain" and
13 "distributed ledger," they tend to often mean
14 the same thing.

15 Q. Okay. For purposes of today's
16 deposition, if I use the terminology "blockchain
17 system," is it -- can we agree that that will
18 also encompass distributed ledger systems?

19 A. I think we just said that all three
20 systems, we can classify them in distributed
21 blockchain. So, yeah, feel free to call them
22 blockchain or distributed ledger. I would go
23 with it.

24 Q. Okay. On the -- still on your CV, at
25 the bottom of page 2, you noted that you were

1 [REDACTED] - Highly Confidential

2 the PC co-chair of three peer-reviewed workshops
3 with published proceedings --

4 A. Yes.

5 Q. -- in the period 2017 to 2019.

6 What does that mean?

7 A. Workshops are typically ranked below
8 conferences and journals in academic quality,
9 which is why I don't list workshops on my CV.
10 When you are PC co-chair -- program committee
11 co-chair, which means that you are, either alone
12 or with other co-chairs, selecting which
13 researchers are going to form a program
14 committee.

15 And what the program committee does
16 then is, that it reviews the papers submitted by
17 other researchers. So like the editor of --
18 you're not the editor but you're organizing
19 other -- you're inviting other researchers to
20 contribute by -- to peer review the submitted
21 papers.

22 So PC co-chair is the person who
23 actually asks and oversee the entire process of
24 the -- of the review process. It invites other
25 researchers to join the program committee.

1 [REDACTED] - Highly Confidential

2 Q. Okay.

3 A. And this is how it works.

4 Q. You mentioned a ranking. Is that --
5 what do you -- what do you mean by that?

6 A. So, I meant that PC co-chairs, for
7 example, they -- if they are co-chairing, they
8 typically look at the process, inviting people
9 to be program committee -- members of the
10 program committee, and make sure that the
11 reviews are detailed enough that they are
12 timely, rather than reviewing the papers
13 themselves.

14 Sometimes, you know, you're jumping
15 into -- if it's needed that there is an
16 additional review, but this is usually not the
17 part of the -- so it's more the -- it's not the
18 hierarchy, it's more the distribution of roles.

19 Q. Okay.

20 A. Yeah.

21 Q. Within scientific literature, what
22 does it mean for a publication to be peer
23 reviewed?

24 A. Yes, so what this means, that there
25 were some peers, usually people who sit on the

1 [REDACTED] - Highly Confidential

2 set program committee, who would read the paper,
3 and accept that this is acceptable in the -- so,
4 it should be published. So basically there is a
5 filter.

6 So program committee, which we
7 discussed, poses a filter and selects, out of
8 submitted papers, a fraction of them. Depending
9 on the quality of conferences, fraction can be
10 bigger or smaller.

11 Q. Are peer-reviewed publications
12 considered to be more reliable than those that
13 are not?

14 A. That's a good question. So, we will
15 need to see by whom. There are some very
16 valuable -- normally you would. In the
17 scientific world, in the academic world, the
18 general answer is yes.

19 This is not the only answer. Why?
20 Because sometimes the impact is measured, for
21 example, by the number of times people cite your
22 work.

23 There are certain cases where people
24 don't publish their work in a peer-reviewed
25 sense. So they publish it, you know, as -- so

1 [REDACTED] - Highly Confidential

2 there is freely accessible and everything, but
3 in the -- they're not peer reviewed. I don't
4 know.

5 One example that comes to mind is the
6 bitcoin's white paper. It was never peer
7 reviewed, this was just out there, but you
8 wouldn't say that this is a bad paper and that
9 it has a small impact.

10 You would look at other metrics, for
11 example, like the number of citations, and it
12 would give you what people -- what impact on
13 thinking and, you know, advancement of human
14 knowledge this has.

15 Q. Okay.

16 A. So in general, yes. In practice,
17 it's -- it's a bit more blurry, yeah.

18 Q. Okay. When you -- when you said
19 "impact," I want to understand; in your mind,
20 what's the relationship between a paper having
21 impact versus being reliable?

22 A. Did you define reliable paper? Which
23 means -- how we define reliable paper? That all
24 the claims in the paper are...

25 Q. Well, what do you think of as a

1 [REDACTED] - Highly Confidential

2 reliable paper?

3 A. So that would be paper that has
4 reproducible results. That has something that,
5 you know, has -- basically comes with research
6 that can be validated by others --

7 Q. Okay.

8 A. -- independently.

9 And this result is reproducible, and
10 so we would call it reliable.

11 There -- there are also -- for
12 example, the difference would be -- between
13 reliable and impactful paper, would be a paper
14 that has a bug, so describes a protocol that has
15 a bug inside, but bug is difficult to discover,
16 it's discovered only years afterwards. But in
17 the meantime, there is a lot of citations to
18 that paper, so the paper is impactful.

19 Q. Okay. Why did you decide to leave [REDACTED]
20 [REDACTED] to become self employed?

21 A. I decided -- so I worked in [REDACTED] since
22 2015, and I worked on blockchain projects. So,
23 you know, we can definitely add permission to
24 blockchain projects, to the space of blockchain
25 projects.

1 [REDACTED] - Highly Confidential

2 And I worked on that, and in my
3 classification of -- and methodology, we'll see
4 a distinction between permissionless and
5 permission blockchains.

6 So while working on permission
7 blockchains, I was one of the coin mentors of
8 [REDACTED]. I'm one of the three
9 original architects of the flow, how that works.

10 And this was meant to be a blockchain
11 that's used for businesses. Right? So, this is
12 just a decentralized -- so this -- this
13 distributed -- some cases, it could be in
14 decentralized -- ledger, which is distributed
15 across multiple companies, and they track
16 certain information. It's like a distributed
17 database which tolerates certain aspects of
18 faults. Right?

19 Companies that participate in these
20 blockchains, they're selected either by
21 consortium, they select each other, they kind
22 of -- so this is where the permissionness of it
23 comes.

24 Whereas in permissionless systems,
25 which are open for participations of anyone,

1 [REDACTED] - Highly Confidential

2 this is a more open system. They are more
3 challenging to design.

4 And, I was trying to actually work on
5 that for a long time. So you see that some of
6 the projects that I mentioned on bitcoin and
7 Ethereum, they were started even while I was
8 working in [REDACTED]

9 So for a while, I was trying
10 internally to make [REDACTED] just a step in the
11 direction of permissionless blockchains, and for
12 different strategical reasons or -- or like
13 orientation if [REDACTED] did -- didn't work.

14 And then I just decided to step out to
15 that space and to work in that space because
16 this is what I like working on.

17 Q. Okay. So would it be fair to say that
18 one of the reasons, or -- or perhaps part of the
19 motivation for leaving [REDACTED] was to focus
20 more of your attention on permissionless
21 blockchain?

22 A. Yes.

23 Q. And would it be fair to say that most
24 of your work while at [REDACTED] focused on
25 permissioned blockchain?

1 [REDACTED] - Highly Confidential

2 A. This is fair to say. Again, I
3 mentioned two projects in -- you know, one paper
4 that came out while I was in [REDACTED] was actually
5 the link between permission blockchains and
6 Ethereum network, and so there was research not
7 constrained only to permissioned blockchains,
8 but -- you know.

9 So, it was -- definitely the larger
10 fraction of the time and larger percentage of
11 time was oriented to permission blockchains,
12 indeed.

13 Q. Can a permissioned blockchain be
14 decentralized?

15 A. It can.

16 Q. So both permissioned and
17 permissionless blockchains could be
18 decentralized?

19 A. They can.

20 Q. Okay.

21 How are you compensated for your work
22 with [REDACTED]?

23 A. I have -- so basically, I have a
24 monthly -- contract with monthly payment in U.S.
25 dollars. And I have certain like compensation

1 [REDACTED] - Highly Confidential

2 in [REDACTED] tokens with a big -- so with a
3 vesting period and everything.

4 Q. Does your compensation with [REDACTED]
[REDACTED] depend in any way on the success of the
6 project, projects you're working on?

7 A. In some sense, it would. Because, you
8 know, you would get the recognition, and you
9 would climb up the certain compensation ladder,
10 or you would be awarded more compensation if you
11 are evaluated as a -- successful.

12 But it's not -- if you asked it's in
13 the contract, it's not in contract. It's
14 more --

15 Q. Okay. Why did you leave academia in
16 2014?

17 A. Ah, that's a good question. So, I
18 left academia because of the so-called two-body
19 problem. In academia, usually my wife is also a
20 researcher. She has a Ph.D. in [REDACTED].
21 And normally if you work in academia, one
22 terrible problem that you have as a family is to
23 find two jobs at the same physical geographical
24 location.

25 So we tried to do it when we were in

1 [REDACTED] - Highly Confidential

2 [REDACTED] My wife was a postdoc in [REDACTED] This
3 is like a big government -- I mean public
4 research institution in [REDACTED] But she has a
5 temporary contract as a postdoc.

6 I was assistant prof-- well, actually,
7 it was professor, but it's not, because it's
8 tenured, which is why I also mentioned tenure.
9 And we had a position there. At some point, she
10 needed to -- she was kicked out -- not kicked
11 out, but her contract --

12 Q. You don't need to -- I don't need to
13 know the details.

14 A. So, I should jump in, then she got an
15 offer from [REDACTED], and I was picking
16 up phone from my, like -- you know, trying to
17 get a position at the same geographical location
18 as her.

19 And I knew people in [REDACTED] because I
20 work there as a postdoc before. I was picking
21 up the phone, saying, Guys, you know, is it okay
22 I come. We were collaborating for a long time.
23 They were, of course, happy.

24 And I went -- it's is more difficult
25 to become at that time -- you know, I'm not sure

1 [REDACTED] - Highly Confidential

2 I could do it now, but I probably have bigger
3 chances than I had at the time.

4 To be a professor at [REDACTED] it's the
5 top thing. It's comparable to being professor
6 at MIT and Stanford University. So it's not
7 easy to just go there and be a professor, right?
8 That's why I went to [REDACTED].

9 Q. Okay. How many people work for you
10 now in your current self employment?

11 A. Myself.

12 Q. Okay. Have you ever run a company?

13 A. I was -- I didn't run a company
14 myself. So I -- I was -- at some point, [REDACTED]

[REDACTED]

[REDACTED]

17 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

21 Q. Okay.

22 So is it -- you've never run a tech
23 startup?

24 A. I never run a tech startup yet, no.

25 Q. Okay. Do you sit on and boards of any

1 [REDACTED] - Highly Confidential

2 technology companies?

3 A. No.

4 Q. Okay.

5 All right. Let's turn -- turning to
6 another topic.

7 I assume you consider yourself to be
8 part of the scientific community?

9 A. I do.

10 Q. What types of professionals, or
11 people, do you consider to be within the
12 scientific community?

13 MR. SYLVESTER: Objection.

14 A. I'm not sure I understand the
15 question. Sorry.

16 Which types of professional is
17 considered part of scientific community.

18 Anybody who follows the scientific --
19 I guess, very broadly, anyone who follows
20 scientific principles, tries to publish papers,
21 you know, following the scientific approach in a
22 repeatable fashion. We -- we discussed this a
23 bit.

24 Normally to get some -- so this could
25 be people who have formal academic education,

1 [REDACTED] - Highly Confidential

2 like Ph.D.s, master's students, but it doesn't
3 really have to be.

4 Q. Okay.

5 When did you first read the 2017
6 Troncoso paper?

7 A. I read it while I was preparing for
8 the -- this deposition. In details, yes.

9 Q. Okay. So, when was that that you
10 first read Troncoso?

11 A. That must be June and July, yes.

12 Q. Of -- of 2021?

13 A. Yes.

14 Q. How did you come to read the Troncoso
15 paper?

16 A. I was searching for -- to formalize my
17 intuitive understanding of what decentralized
18 systems mean. And I was looking through the
19 literature to understand if somebody had done
20 this before.

21 It's easier, much, much easier,
22 much -- in some sense -- well, easier to
23 convince other people, right, if you find the
24 prior art which did it.

25 So I was doing this, and the one of

1 [REDACTED] - Highly Confidential

2 the papers that stand -- stood out because it
3 systematized 15 years, as the title says, of
4 research and decentralization and privacy, was
5 that paper.

6 Since I know Carmela Troncoso, and
7 George Danezis, so I know them. So, this was a
8 paper that stood -- ah, these are the people
9 whose opinion I value. They're very well known
10 researchers in the community.

11 Q. How do you know Carmela Troncoso?

12 A. While we were working in [REDACTED] on COVID
13 passports, she was -- we were proposing a
14 [REDACTED] blockchain-based solution for
15 basically how COVID passes work today. This was
16 one of the ideas I contributed in March last
17 year.

18 And we were developing a blockchain
19 solution, and Carmela Troncoso -- whilst we
20 talked to Swiss government to adopt this
21 solution for their COVID pass, Carmela Troncoso
22 was on the board that reviewed the solution.

23 Q. Have you discussed this -- your work
24 in this case with Carmela Troncoso?

25 A. No, I did not.

1 [REDACTED] - Highly Confidential

2 Q. Okay. The Troncoso paper, by the way,
3 that we've been referring to, is Reference 21 in
4 your report. Correct? On page 30.

5 A. Yes, it is.

6 Q. The -- that reference, 21, lists the
7 other authors. Which of other authors of that
8 paper do you know personally?

9 A. I spoke to George Danezis.

10 Q. When did you speak to him?

11 A. September or -- August or September.
12 This year.

13 Q. Of 2021?

14 A. Yes.

15 Q. What did you discuss with him?

16 A. Collaboration, because the -- George
17 Danezis is a very well-known researcher in the
18 blockchain space. He worked for many blockchain
19 projects, including Facebook's -- or Meta's --
20 Libra or Diem project, and I was trying to get
21 him on board that we collaborate on the same
22 projects.

23 Which you could call, these are the
24 projects that I do in the context of [REDACTED]
25 [REDACTED] but as you see, this is in the whole

1 [REDACTED] - Highly Confidential

2 decentralized computing research space, so we
3 were discussing the possibilities if we
4 collaborate together.

5 Q. Did you talk to Mr. Danezis about your
6 work on this case?

7 A. No.

8 Q. Did you talk to Mr. Danezis about your
9 plans to cite the Troncoso paper?

10 A. No.

11 Q. You said earlier this morning that the
12 Troncoso paper itself had a motivation of -- of
13 coming up with a definition of decentralization
14 because there was no consensus at that point.
15 Is that right?

16 MR. SYLVESTER: Objection.

17 A. One of the lines in the paper is that
18 the motivation of the paper is that there are
19 different definitions of the decentralization.
20 And this was one of the motivating points for them
21 to, in 2017 or earlier -- you usually do the
22 research a bit earlier than -- than when the
23 paper is published -- that they -- I guess like
24 I'm giving an expert opinion here because fixing
25 this is important for people, and they started

1 [REDACTED] - Highly Confidential

2 looking, like few years ago, including Troncoso.

3 So at that moment we could say that it was not

4 as clear as today what this means.

5 Q. Is -- today as you sit here, do people

6 in the scientific community use the term,

7 "decentralized," consistently, in discussing

8 distributed systems?

9 MR. SYLVESTER: Objection.

10 A. Can you define "consistently"? Do

11 they use the very same wording? Probably not.

12 Do they think the same thing? That's a

13 different thing. Well, what do you mean by

14 "consistent"?

15 Q. Well, do you -- do you believe that

16 there is consensus in the scientific community

17 about the proper way to define decentralization

18 in blockchain systems?

19 A. I think there is a consensus on what

20 is the minimum. If not explicit/there is

21 certainly -- there is certainly. To my

22 understanding, there is implicit consensus of

23 what requires the basic or minimum definition or

24 if you want the necessary definition for a

25 system to be considered decentralized.

1 [REDACTED] - Highly Confidential

2 Q. What are you referring to there?

3 What -- what is -- what do you think there is
4 consensus about?

5 A. So the minimal conditions that a
6 the -- that system needs to satisfy in order to
7 potentially be called decentralized. So, people
8 might differ, right, if this is not satisfied, I
9 don't know if any expert, my colleague, or
10 anyone who would call the system decentralized
11 even if this -- basic definition is not
12 satisfied.

13 Then again, some might put the bar
14 higher. So even if you pass this basic
15 definition, some people would probably not still
16 call it decentralized because you're not passing
17 the higher bar. And the bar that we are
18 discussing is the Troncoso definition.

19 Q. So, based on what you just said,
20 doesn't that mean that people in the scientific
21 community still today have not reached consensus
22 on where to place the bar on decentralization?

23 MR. SYLVESTER: Objection.

24 A. It's -- I said, so they can -- there
25 is -- to my understanding, there is a consensus

1 [REDACTED] - Highly Confidential

2 on the minimal condition.

3 Q. What is the consensus?

4 A. So, this is -- the fact, the fact,
5 this is the -- to my understanding, no one would
6 call the system -- no researcher who considers
7 him an expert in the field would call a system
8 decentralized, even if it does not satisfy the
9 Troncoso definition.

10 Let's me put this way.

11 Q. What is the minimum condition for
12 decentralization that you think there's
13 consensus about?

14 A. That there is no single authority
15 trusted by all, in the system. In a distributed
16 system with authorities controlled by different
17 parties, so with components controlled by
18 different authorities or different parties,
19 there must not be the one which is fully trusted
20 by all.

21 I don't know if anyone who would call
22 a system decentralized which does not satisfy
23 this. Which means, you get a system in which
24 there is a party which is fully trusted by all,
25 and you get an expert who says, This system is

1 [REDACTED] - Highly Confidential

2 still decentralized even though there is a party
3 which is fully trusted by all.

4 This would be negating the Troncoso
5 definition and still -- still calling the system
6 decentralized, I think there is a consensus that
7 this is not case.

8 Q. Is it your position that the
9 scientific community has reached consensus that
10 Troncoso's definition of decentralization is the
11 correct one?

12 A. I didn't say that. So you can phrase
13 what I said in different ways.

14 For example, one of the papers that --
15 for example, Adriaens, Professor Adriaens cited
16 in his rebuttal, it's not citing Troncoso but
17 it's using the same definition, same wording,
18 of -- what I just said, to say whether -- which
19 system is decentralized.

20 It's not even citing Troncoso, but
21 it's using the same wording. So, you know, if
22 you ask whether, word for word, Troncoso
23 definition is consented upon, that's probably --
24 we can discuss that, but the essence of it is --
25 what's emerging is the -- what emerged as a

1 [REDACTED] - Highly Confidential

2 minimal definition of decentralization.

3 So you need to pass the definition in
4 order to be called decentralized. Some people
5 might call -- still call it centralized, even if
6 you pass the definition.

7 Q. Dr. [REDACTED] did you speak at the

8 [REDACTED]

[REDACTED] --

10 A. I did.

11 Q. -- [REDACTED]?

12 A. I did.

13 Q. Do you recall -- and there's a --
14 there's a [REDACTED]

16 A. Not of my remarks but of my talk, yes.

17 Q. Of your talk.

18 A. Yes.

19 Q. Do you recall stating, [REDACTED]

[REDACTED], that you had an
21 impression there was no consensus in how to
22 define decentralization, but then you found a
23 nice PETS paper by Carmolo -- Carmela Troncoso
24 and others.

25 A. I don't recall the -- the exact

1 [REDACTED] - Highly Confidential

2 wording, sorry.

3 Q. Okay. Let's play it for you.

4 And I think the way we'll do this
5 is -- because of the limitations here, I don't
6 think we can put it on the screen.

7 Can we? You want to try?

8 MR. FORD: I could, but it would get
9 rid of the Webex.

10 MS. ZORNBERG: Okay. Why don't you
11 just take it over there and show
12 Dr. [REDACTED]

13 We're going to -- Exhibit 33 is the
14 clip that we'll show you from your -- from
15 you [REDACTED]
[REDACTED]

17 (Recording played.)

18 A. You can stop it. Thank you. Very
19 good. So...

20 Q. So let me -- let me put the question.

21 Having watched the video clip, do you
22 agree that you said, on [REDACTED], I had
23 an impression that there was no consensus in how
24 do you define decentralization. Then I found a
25 nice PETS paper by Carmela Troncoso and others.

1 [REDACTED] - Highly Confidential

2 And you go on.

3 Is that accurate?

4 A. That I say. I said that, yes.

5 Q. Okay. So, did you -- would you agree
6 that, at a minimum, until you found the Carmela
7 Troncoso paper, which you said occurred in June
8 or July of 2021 -- before that time, you had the
9 impression that there was no consensus in how to
10 define decentralization?

11 A. I was -- that is fair.

12 That is fair --

13 Q. Okay.

14 A. -- to say. Yes.

15 Q. So, since finding the Troncoso paper
16 in June or July of 2021, what have you done to
17 determine whether others in the scientific
18 community also adopt the Troncoso definition?

19 A. When I -- basically -- they don't need
20 to adopt it. Again, we discuss that somebody
21 can put the bar higher. When you put the bar
22 higher, there are papers who require you, you --
23 a blockchain system to be called decentralized,
24 to work with honest majority -- or something
25 like that -- by allow -- allowing that a

1 [REDACTED] - Highly Confidential

2 minority of parties is considered Byzantine. So
3 that's higher a bar.

4 So if you're allowing, you agree with
5 me. So if you have a Troncoso definition, you
6 would have these things.

7 But in order for Troncoso definition
8 to be minimal, and I like that it's very
9 permissive, it's very general, it admits a lot
10 of systems so the not bar is not set high so
11 it's debatable.

12 What I liked is that it puts the bar
13 very low and goes into the essence of trust in a
14 single authority. So I was -- and actually,
15 that was my understanding.

16 If you ask me if I wrote the report
17 without actually looking -- refreshing like what
18 happened in last four years, this would be my
19 definition. I would actually not put the bar
20 higher because I don't think this is fair.

21 For example, I mention -- in the rest
22 of the talk, I mention the four-node BFT
23 protocol. This is a permission system that runs
24 on four nodes and tolerates any malicious party
25 among them.

1 [REDACTED] - Highly Confidential

2 It's a closed system with closed
3 membership, and I was -- I think -- I still
4 think it's fair to call it decentralized.

5 Q. Okay.

6 A. Now, when I saw -- when I looked at
7 the Troncoso definition, I was like, Okay. So,
8 I mean, before I looked at this from the -- from
9 the formal perspective, I thought -- and it was
10 open.

11 When I -- when I -- when I started
12 writing about methodology, one possible outcome
13 was that we still didn't come up to the minimal
14 definition, as a scientific community. That
15 could be one outcome.

16 So, while I was doing that -- and I
17 didn't write the report, so that was one
18 possible outcome.

19 Now, when I started diving into the
20 literature, I saw that people had been looking
21 into this, and the bar is actually set very low.

22 And -- yeah. And I couldn't find the
23 definition, I couldn't find any definition which
24 goes against -- that, again, would admit a
25 system is decentralized if it does not satisfy

1 [REDACTED] - Highly Confidential

2 Troncoso definition.

3 So we are talking about a system in
4 which there is single authority which is trusted
5 by all, and you call that thing decentralized.

6 Q. What alternative definitions of
7 decentralization, besides Troncoso, did you
8 consider when you dove into this subject in the
9 summer of 2021?

10 MR. SYLVESTER: Objection.

11 A. So, one of the papers that I cite in
12 my report, which is the paper by Sai and others,
13 it puts the bar high. So basically discusses
14 decentralized systems, which require an honesty
15 majority.

16 So basically with any honest majority,
17 the system would still be called decentralized,
18 which means that it tolerates dishonest
19 minority. That puts the bar higher.

20 Q. Okay. If fewer than all participants
21 in a system trust only one party, would you
22 degree that's not centralized?

23 A. I think you are getting something
24 wrong. At least in my -- from my brain. Can
25 you repeat, please?

1 [REDACTED] - Highly Confidential

2 Q. If fewer than all participants --
3 sorry.

4 A. Yes.

5 Q. If fewer than all participants trust
6 any one party, would you agree that's not
7 centralized?

8 A. If I and all other participants, we
9 trust the same party, would I agree that this is
10 not centralized.

11 No?

12 Q. Rephrase it. Rephrase it.

13 A. I would say -- so the way I understand
14 your system here is, driving, I would say it's
15 centralized and not decentralized.

16 Q. Before you settled on the Troncoso
17 definition in your report, with whom did you
18 discuss the definition of decentralization?

19 MR. SYLVESTER: Objection.

20 A. I was reviewing and discussing with
21 myself. I'm giving opinions, so I'm consulting
22 the literature and -- yeah.

23 Q. Okay. Now, the Troncoso definition
24 refers to decentralized distributed systems
25 having multiple authorities that control

1 [REDACTED] - Highly Confidential

2 different system components.

3 A. Yes.

4 Q. Right?

5 Might those multiple authorities
6 provide updates to the system components over
7 time?

8 A. You mean can they change software on
9 which they're running or --

10 Q. Yes.

11 A. They can.

12 Q. Can they improve the system components
13 over time?

14 A. They can.

15 Q. Can the multiple authorities fix bugs
16 in the system over time?

17 A. It depends on how the system -- if
18 it's an open-source system and depending on the
19 governance of that open-source project, they
20 could. They -- in some cases, they might not be
21 able to because they don't have the rights. It
22 depends.

23 Q. Okay. Does the fact that multiple
24 authorities can provide updates to the system
25 over time affect whether the system is

1 [REDACTED] - Highly Confidential

2 decentralized?

3 A. Again, to -- in my report, and the way
4 I think about this systems, you need to fix the
5 software before you call it decentralized or
6 not.

7 What these authorities in your example
8 would be allowed to do is to change their own
9 copy. If I am running a validator node on
10 blockchain X, I could change my validator, and
11 this is the -- so change and basically put any
12 code that I want to run there. That I can do,
13 even with the fixed code of others.

14 Then if I'm doing that, I'm trying
15 to -- I'm considered Byzantine because I'm not
16 playing by the set rules.

17 What's important is that that -- at
18 that moment, the system maintains property not
19 with respect to me because I violated the
20 contracts by running the code that's -- that I'm
21 not supposed to run, but I'm not supposed to
22 influence others.

23 So you -- these nodes are usually
24 caused the honest nodes. Does this answer your
25 question?

1 [REDACTED] - Highly Confidential

2 Q. Not quite. But let me -- let me ask
3 it again.

4 We agree that multiple authorities, in
5 certain blockchain systems, can contribute to
6 updates to the system that do get accepted into
7 the protocol over time?

8 A. We need to fix -- again, we need to
9 fix the software version, and then discuss its
10 decentralization.

11 Once we do that, we need to exclude
12 your case where you propagate updates to others,
13 because we need to -- so we need to take a
14 snapshot. You can make a decentralized system
15 centralized by code changing. You can make a
16 centralized system decentralized by code
17 changing. You have to do both.

18 Q. You can do both?

19 A. You can do both.

20 Since we can do both, you need to take
21 a snapshot in time, stop software changes that
22 you propagate to others that others adopt, and
23 basically focus on that particular software, and
24 maybe changes -- if you're a Byzantine node
25 untrusted by others, you are allowed to change

1 [REDACTED] - Highly Confidential

2 the -- your software that you are running
3 however you want. But that's your software.
4 You are not propagating the changes to others.

5 Q. Okay. Troncoso says that all parties
6 must trust one authority --

7 A. It doesn't say that.

8 Q. -- for the -- well, I didn't finish
9 the question.

10 A. I'm sorry.

11 Q. If a system is set -- in a centralized
12 system, Troncoso says that all parties must
13 trust one authority?

14 A. This is not -- so there must --
15 negation of the property will say there exist
16 authority which is trusted by all.

17 Q. One authority trusted by all?

18 A. At least one.

19 Q. Okay. So my question is, if fewer
20 than all parties trust any one authority, does
21 that meet Troncoso's definition of
22 decentralized?

23 A. No.

24 Q. Why not?

25 A. We used it in centralized. We just

1 [REDACTED] - Highly Confidential

2 negated the Troncoso defi-- the Troncoso says no
3 parties fully trusted by all. If you have a
4 party which is trusted by all, that negates the
5 definition.

6 Are you -- do you agree?

7 Q. If fewer than all parties trust --

8 A. Fewer than all --

9 Q. -- one --

10 A. -- fewer than all parties. Okay.

11 Q. -- then do you agree that meets the
12 Troncoso definition of decentralization?

13 A. If --

14 Q. I'm sorry, did you answer?

15 A. Yes, yes, yes, I'm thinking.

16 So you could build systems like that.

17 That -- that could -- that could happen, yes.

18 That could be allowed by the -- by the
19 definition, yes.

20 Q. Okay.

21 All right. You mentioned the Sai
22 paper. We've marked it as Exhibit 4.

23 (Sai paper was marked [REDACTED] Exhibit 4 for
24 identification, as of this date.)

25 Q. And the Sai paper is a paper you

1 [REDACTED] - Highly Confidential

2 repeatedly recite -- repeatedly cite in your
3 report as Reference Number 17 in your reference
4 list. Right?

5 A. Yes.

6 Q. I'm going to refer to it, Exhibit 17
7 as the Sai paper, or Sai.

8 Are you aware that this is a
9 peer-reviewed -- this paper was published in a
10 peer-reviewed academic journal?

11 MR. SYLVESTER: Sorry, Lisa, the Sai
12 paper that I'm looking at is marked [REDACTED] 4.

13 MS. ZORNBERG: Oh, thank you for the
14 correction. It's Reference Number 17 in
15 Dr. [REDACTED] report, but we're marking it
16 here as Exhibit [REDACTED] 4. Thank you. Thank
17 you.

18 Q. Okay.

19 Looking at Exhibit 4, Dr. [REDACTED] are
20 you aware that this paper was published in a
21 peer-reviewed academic journal?

22 A. Yes, I am.

23 Q. Okay. And the purpose of the Sai
24 paper was to conduct a systematic review of
25 academic literature that discussed

1 [REDACTED] - Highly Confidential

2 decentralization to --

3 A. In public block-- blockchain systems.

4 Q. In public blockchain systems.

5 A. As the name says, yes.

6 Q. Okay. And in the abstract of paper,
7 it references that Sai reviewed 89 research
8 papers published between 2009 and 2019, to
9 arrive at a taxonomy of centralization.

10 MR. SYLVESTER: And, [REDACTED] if you
11 don't recall, take your time to take a look
12 at the paper to answer her question.

13 A. Yes.

14 I -- at some point, I need to go to
15 the toilet.

16 Q. Then why don't we take a break now?

17 A. Is this the right time.

18 Q. Yeah, it's fine. It's totally fine.

19 A. Okay. Thank you.

20 THE VIDEOGRAPHER: The time is
21 10:52 a.m. We're going off the record.

22 (Recess from 10:52 to 11:10.)

23 THE VIDEOGRAPHER: It is 11:10 a.m.

24 We are back on the record.

25 Q. Dr. [REDACTED] a little while ago we

1 [REDACTED] - Highly Confidential

2 were speaking about permissioned and
3 permissionless blockchain systems. What is a
4 permissioned blockchain system?

5 A. Permissioned blockchain system is, in
6 a nutshell, a system in which you cannot join
7 without permission of some entity. This can be
8 a centralized entity. This can be a
9 decentralized entity, like current members in
10 the system could vote to admit another one into
11 the system and so on.

12 As opposed to that in permissionless
13 systems, this permission is not necessary. So
14 you would just -- if you want to run a validator
15 in a -- in some kind of blockchain effort, you
16 would download the code. You would join the
17 game, start validating transactions.

18 Q. You said earlier that a -- a
19 permissioned system can be either centralized or
20 decentralized. Correct?

21 A. Yes.

22 Q. Can you give an example of a
23 decentralized permission system?

24 A. So we could -- if you have four
25 validator nodes, and they run a consensus

1 [REDACTED] - Highly Confidential

2 protocol and they tolerate any malicious action
3 of any one of them. So usually -- I mean,
4 depending on the failure thresholds, this number
5 of Byzantine nodes that tolerate is less than
6 one-third of nodes, sometimes one-half of nodes.
7 And usually in the literature, that depends --
8 so this is the best you can do.

9 And that distinction, whether it's one
10 or the other, it depends on network assumptions,
11 how timely is the network, which means if I send
12 a message to you, is it delivered in, like,
13 limited amount of time? So does every message,
14 for example, take up to two seconds, not more,
15 for me to reach you? If it takes more and
16 albeit a long time -- we talk about asynchronous
17 network. So if network is asynchronous or
18 synchronous, these bounds --

19 Q. If a network?

20 A. Is asynchronous -- asynchronous or
21 synchronous --

22 Q. I don't know that word.

23 A. If it takes unbounded amount of -- so
24 I send -- so my computer is sending --

25 THE COURT REPORTER: I'm not hearing

1 [REDACTED] - Highly Confidential

2 your words now.

3 THE WITNESS: Okay. Sorry.

4 THE COURT REPORTER: If it takes what?

5 A. If it takes unbounded amount of time
6 and for -- in the worst case, for my message to
7 reach to you, which means that probably on the
8 network there are some network outages, network
9 partitions, so maybe there are, like, you know,
10 cable under water, cable is broken down and
11 somebody needs to repair it, and I keep trying
12 to reach you and only eventually my message
13 reaches. And this time period is unbounded. We
14 are talking about asynchronous network.

15 Q. Can you spell that word?

16 A. Asynchronous.

17 Q. Spell that.

18 A. A, like letter A, synchronous.

19 Q. Asynchronous?

20 A. Yes, asynchronous. Yes.

21 Q. Okay. Thank you.

22 A. Sorry. Anyways, so depending on the
23 underlying network assumptions, Byzantine fault
24 tolerance protocol, which can be used in the
25 permission blockchain systems, tolerates less

1 [REDACTED] - Highly Confidential

2 than one-third of the total number of nodes or
3 less than one-half.

4 This can be smaller. This can be less
5 than one-fifth or so on.

6 But these are usual bounds that
7 appear. So if I have four nodes, four validator
8 nodes, I could come up with a -- Byzantine
9 Fault-Tolerant protocol that tolerates to
10 certain extent; and there are technical details
11 what the certain extent means, this asynchronous
12 network.

13 And it tolerates any Byzantine
14 behavior of any one of them. But if two of them
15 misbehave, they could break the safety and
16 liveness properties.

17 So why is this decentralized? Because
18 we could have four nodes and not any one is
19 trusted by all. Actually, not any one is able
20 to subvert the key proprietors of the system.
21 Then basically, this would qualify under
22 Troncoso definition as a decentralized network.

23 Q. Okay.

24 A. So in that sense, the Troncoso
25 definition sets the bar pretty low. This is

1 [REDACTED] - Highly Confidential

2 what I mentioned before.

3 Q. Okay. So I would like you to take a
4 look at Exhibit 4, which is the Sai paper.

5 A. Yes.

6 Q. Does the Sai paper cite to the
7 Troncoso definition of decentralization that you
8 adopted in your report?

9 A. It does not. What it does, it
10 provides a stronger definition of
11 decentralization.

12 Q. Okay. Is it fair to say that Sai
13 surveyed 89 research papers over a ten-year
14 period, to address the taxonomy of
15 centralization, and it did not cite Troncoso,
16 among those 89 research papers?

17 A. It is fair to say that they did it,
18 yes.

19 Q. And in your own published writings
20 before 2021, have you ever cited to the Troncoso
21 paper?

22 A. I did not.

23 Q. I want to direct your attention to the
24 abstract on the first page, of the Sai report.

25 Around midway down, where it -- the

1 [REDACTED] - Highly Confidential

2 Sai paper states, quote, Our study contributes
3 to the existing body of knowledge by
4 highlighting the multiple definitions and
5 measurements of centralization in the
6 literature.

7 Closed quote.

8 Do you see that?

9 A. Our study contributes to the existing
10 body --

11 Yes.

12 Q. Okay. The Sai paper was published in
13 2021 --

14 A. Uh-huh.

15 Q. -- right?

16 A. Yes.

17 Q. Yes? And do you agree that Sai, at
18 least, states that the literature includes
19 multiple definitions and measurements of
20 centralization?

21 A. By highlighting the multiple
22 definitions and measurements of centralizations,
23 yes, he says that in the abstract.

24 Q. Do you agree that as of when the Sai
25 paper was published, there were multiple

1 [REDACTED] - Highly Confidential

2 definitions and measurements of centralization
3 in the scientific literature?

4 A. Clearly, there are still even after.
5 If you take Sai paper, it proposes a different
6 definition of centralization than Troncoso. So
7 the answer is yes.

8 Q. Okay.

9 I would like to direct you to your
10 report to the top of page 5.

11 And the top bullet, you wrote, quote,
12 I adopt the basic definition of a decentralized
13 system as defined by Troncoso, et al.

14 Closed quote.

15 Did I read that correctly?

16 A. Yes.

17 Q. Was it your intention in the report to
18 present the Troncoso definition of
19 decentralization as the authoritative definition
20 in the scientific community?

21 A. I -- my intention was to refer to it
22 as I did, as a basic definition of a
23 decentralized system.

24 Q. Why --

25 A. In more mathematical terms, this

1 [REDACTED] - Highly Confidential

2 could -- at some point I call it minimal. I
3 refer to it as minimal. And you can think of it
4 as necessary.

5 In mathematical terms, necessary and
6 sufficient is -- it's necessary. I'm adopting
7 it as a necessary definition.

8 Q. Why did you describe it as "the basic
9 definition," instead of "a basic definition"?

10 A. Can we attribute it to my English?
11 But -- English is not my first language. I
12 normally have issues with -- with these things.

13 Q. Did you mean to suggest in your report
14 that the Troncoso definition is the only basic
15 definition of a decentralized system?

16 A. Again, it's -- what I think is that
17 it's necessary. If you don't -- when I say
18 "basic," what I mean is necessary. If a system
19 does not satisfy the -- this definition,
20 according to my understanding, my expertise, my
21 understanding of this field, and backed by all
22 the evidence that's written here, including the
23 Troncoso definition, I would say that this, such
24 system could not be qualified as decentralized
25 and, hence, it's centralized.

1 [REDACTED] - Highly Confidential

2 Q. But would you agree -- would you
3 agree, Dr. [REDACTED] that there are other
4 definitions of decentralized systems that you
5 can find in the scientific literature?

6 A. You can -- one can find different
7 definitions of decentralization in the
8 scientific literature, none of which, to my
9 understanding, would admit a system is
10 decentralized, if it follows Troncoso
11 definition. Do you see the -- where I'm going
12 with "basic" and "minimal"?

13 Q. So your position is that there is no
14 definition in the scientific literature of
15 "decentralization" that doesn't have the
16 Troncoso definition as a basic minimum?

17 A. To my understanding, there is no
18 definition of decentralization. And certainly I
19 didn't see any -- and I doubt it exists -- that
20 would admit a system is decentralized if it
21 doesn't satisfy Troncoso definition.

22 Q. Did you consider the definition of
23 decentralization provided in a 2020 paper by
24 Keke Wu, spelled K-E-K-E, W-U, title "A
25 Coefficient of Variation Method to Measure the

1 [REDACTED] - Highly Confidential

2 Extents of Decentralization for Bitcoin and
3 Ethereum Networks"?

4 A. Do you have that paper as a exhibit?

5 Q. No, not right now.

6 But is that -- are you familiar with
7 that paper?

8 A. I'm familiar with that paper, yes.

9 Q. When did you review it?

10 A. I reviewed it after Adriaens'
11 rebuttal.

12 Q. Okay. So I'll just read you one
13 sentence from the paper where it Wu wrote that
14 in blockchain systems, and I'll quote it, quote,
15 Decentralization means that no single individual
16 can destroy transactions in the network, and any
17 transaction request requires the consensus of
18 most participants.

19 Closed quote.

20 A. Do you have that paper in front of
21 yourself?

22 Q. I don't have it here right now.

23 But --

24 A. Okay. So this is the thing. This is
25 what Adriaens points out in his rebuttal.

1 [REDACTED] - Highly Confidential

2 Unfortunately, he skips -- and this is what
3 Adriaens does in his rebuttal. He takes things
4 out of the context.

5 That very same paper. Section 2, if
6 I'm recalling like -- don't take my -- because I
7 don't have it in my head.

8 But Section 2, Subsection B, it opens
9 with the definition of "decentralized systems,"
10 which is the same as Troncoso definition.

11 Q. Okay.

12 A. We can have -- so -- I mean, I don't
13 have the paper before me.

14 But what it does, it discusses -- so
15 it cites the early work of Baran from 1960s and
16 it points out to Vitalik Buterin's blog post to
17 basically define in the same way -- I'm not
18 saying word for word, but almost the same words
19 because it talks about single authorities fully
20 trusted by all. As Troncoso does.

21 Adriaens doesn't point --

22 Q. What are --

23 A. Adriaens doesn't point that out in his
24 report. And he skips, so that's not a
25 definition. So that particular paper to which

1 [REDACTED] - Highly Confidential

2 you are referring to opens the definition of
3 "decentralization" in the decentralization
4 section by having the same wording or almost the
5 same exact wording as Troncoso.

6 Q. All right. Let me direct you back to
7 the top of page 5 of your report.

8 A. Yes.

9 Q. So in the first bullet which we looked
10 at, you say, I first adopt the basic definition
11 of a decentralized system as defined by
12 Troncoso.

13 And then in the very next bullet, you
14 wrote, quote, I then refined this basic
15 definition.

16 Closed quote.

17 And it goes on.

18 A. Yes.

19 Q. Why did you see a need to refine
20 Troncoso's definition of "decentralization"?

21 A. That's -- that's a good point. So,
22 for example, Sai paper and multiple other
23 papers, they would try to understand, which
24 system is more centralized and which system is
25 more decentralized. They most often focus on

1 [REDACTED] - Highly Confidential

2 bitcoin and Ethereum more.

3 So if you look at bitcoin and
4 Ethereum, the -- the way I treated them in my
5 report, they would both pass Troncoso
6 definition.

7 But still, people would be discussing
8 which one is more decentralized than the other.

9 So if you want, with this methodology,
10 there is one definition which sets the bar very
11 low. And I'm actually surprised, if I may make
12 a comment, that we are discussing this because
13 the aspiration of Ripple consensus, the way it
14 was written, is to be a Byzantine Fault-Tolerant
15 protocol and to actually pass the Troncoso
16 definition easily. It's just that it doesn't.
17 So I'm surprised that we are questioning --

18 Q. I'm sorry. I didn't -- I didn't catch
19 what you said. To pass the Troncoso test, you
20 said, is easy?

21 A. It would be if Ripple was actually a--
22 Byzantine Fault-Tolerant protocol that tolerates
23 Byzantine -- Byzantine fault of any component in
24 that system, it would pass Troncoso definition.

25 It's just that it doesn't. It's

1 [REDACTED] - Highly Confidential
2 marketed as such. But it basically hides
3 extreme complexity in the dUNL membership
4 series. So that's -- if you want, when you
5 design these protocols, this is the most
6 challenging part. And you're hiding it in a --
7 in the -- you're hiding the complexity by having
8 the trusted service that ships the UNL others.

9 Q. Is it -- is it your position,
10 Dr. [REDACTED] that the XRP Ledger fails to meet
11 the Troncoso test because of the way the dUNL,
12 what you call the dUNL, operates?

13 A. This is what I point -- this is the
14 main reason.

15 Even with that fixed, there could be
16 other reasons. Other reasons are pointed in my
17 Appendix B, which are not necessary for my
18 opinion, as I stated my report, because of the
19 main problem is how dUNL operates.

20 Q. Okay. Do you consider
21 decentralization to be binary such that a system
22 is either completely decentralized or completely
23 centralized?

24 A. I -- in my methodology and in this --
25 assuming that we would find a definition that

1 [REDACTED] - Highly Confidential

2 admits a system is decentralized, so this is
3 where Troncoso definition comes. I think this
4 is the bar which says this is either centralized
5 or some people might call it still centralized
6 or decentralized if you pass that filter of
7 Troncoso, so you are satisfying Troncoso
8 definition.

9 I would call it decentralized -- being
10 very generous, I would call it decentralized in
11 this methodology. We'd call it decentralized.
12 Then probably you could find other expert who
13 would say, No. No. No. Wait, wait. Wait.
14 It's not sufficient that it passes Troncoso
15 definition. Let's still see. And there are
16 these different aspects of -- that I discuss in
17 my report, and they -- the others discuss.

18 Q. So why did you feel the need to refine
19 Troncoso's definition of decentralization?

20 A. This is mostly -- I was asked to opine
21 on bitcoin and Ethereum. So, you know, if you
22 have bitcoin and Ethereum, you -- there are
23 certain aspects of them that influence, like
24 this one is more decentralized, and this one is
25 less decentralized. They are decentralized,

1 [REDACTED] - Highly Confidential

2 according to Troncoso definition.

3 And the way the -- not only because of
4 Troncoso definition, because the way current
5 system -- current software operates and current
6 circumstances in the world in which the network
7 operates, they allow them to pass Troncoso
8 definition.

9 Now, it's also when you build a
10 methodology, it's supposed to be able to
11 distinguish different aspects of
12 decentralization. As they are presented in the
13 literature, you will see that my methodology
14 that I adopt very much looks like different
15 measurements and aspects of centralization that
16 Sai has.

17 To be able to evaluate once you pass
18 Troncoso definition, which system is more
19 decentralized than the other.

20 Q. So do I understand correctly, you're
21 saying that you view the Troncoso definition as
22 the bare-minimum definition for
23 decentralization; but beyond that,
24 decentralization can move along a continuum?

25 A. That's a fair way to put it, yes.

1 [REDACTED] - Highly Confidential

2 Q. Okay. And so would you agree
3 decentralization in a blockchain system can
4 change over time?

5 A. It can certainly change with the
6 change in the software. We discussed this
7 already. That's certainly the case. Yes.

8 It doesn't depending only on changes
9 in software but changes in the whole
10 circumstances of the Newark and et cetera. It
11 can change in time.

12 Q. What factors could contribute to a
13 blockchain system becoming more centralized over
14 time?

15 A. Convergence to -- again, in the -- in
16 the world of Troncoso definition, if this is the
17 minimum bar, you want to stay away from the
18 world in which a single authority needs to be
19 trusted in order for other entities in the
20 systems, other authorities or participants in
21 the system to maintain the desired properties of
22 the system. Desired properties in my report are
23 referred as safety and liveness and usually in
24 distributed computing.

25 Q. Okay.

1 [REDACTED] - Highly Confidential

2 THE COURT REPORTER: Usually what?

3 A. Usually in distributed computing.

4 Q. What factors could contribute to a
5 blockchain system becoming more decentralized
6 over time?

7 A. So this -- what can contribute is
8 ensuring that there is no such part that
9 controls vital parts of the system. And you
10 usually do it by -- one way to do it, I --
11 rather than usually. One way to do it is to let
12 go of power, let go of any specific thing that
13 this entity is doing that others are not.
14 Right?

15 Q. Uh-huh.

16 A. So example would be, one of the
17 steps -- I'm not saying if -- if XRP Ledger does
18 it, but one the steps toward such a world would
19 be removing validator list sites completely from
20 the code. That's an example. I'm not saying
21 that's sufficient, but that's a step there.
22 Because suddenly, you would go to the world in
23 which no one is really favored over the other,
24 by its own inclusion to DNLs, you're removing
25 that.

1 [REDACTED] - Highly Confidential

2 Q. In your view, does a blockchain system
3 that includes -- let me rephrase.

4 Is it your position that by including
5 any validator list in the rippled code, that
6 automatically renders the ledger centralized?

7 A. I didn't say that.

8 Q. So explain what you're saying. Can --
9 can the rippled code include any validator list
10 and still be decentralized?

11 MR. SYLVESTER: Objection.

12 A. I would need more time to -- you're
13 speculating on -- on possible future.

14 So we are speculating on changes of
15 the code that happened, and I would need to
16 review them carefully.

17 Q. I'm not -- I'm not sure -- maybe I --
18 I wasn't clear in my question.

19 Even under the version of the code
20 that you reviewed where there's -- I'm asking
21 you, ideologically, do you have a belief that by
22 having any validator list in the rippled code,
23 that mere fact renders the ledger decentralized?

24 MR. SYLVESTER: Objection.

25 A. Again, I'm not saying that. What I

1 [REDACTED] - Highly Confidential

2 said is, you're asking to -- me to opine on
3 something that I didn't write in my report.

4 Whether -- I believe it is possible --
5 let me put it this way. I believe it is
6 possible to have similar concepts that are --
7 that the designers of the protocol tried to
8 express but just implemented in a different way,
9 which would yield a decentralized system.

10 Does that help?

11 Q. Your report does talk about the fact
12 that the rippled code has a validator list in
13 it, a UNL list in it, correct?

14 A. Yes.

15 Q. And I thought the central view
16 expressed in your report is that it's the
17 existence of that Ripple-published UNL that, in
18 your view, renders the ledger centralized.

19 MR. SYLVESTER: Objection.

20 A. No, it is not. This is not what I
21 wrote.

22 Q. So then explain.

23 A. What is rendered centralized is the
24 ability of a validator list site, of the
25 validator list site as of 1.7.3, to serve

1 [REDACTED] - Highly Confidential
2 different UNLs to different. So if -- it's --
3 it needs to be trusted not to do what I'm just
4 describing. If it does serve different UNLs
5 completely -- let's say completely different
6 UNLs, to completely different nodes, what it
7 does, it puts these validators that did get
8 different list out of consensus. They cannot
9 reach consensus without one another.

10 I mean, they could. But, like, the
11 chances that they do not are really real. So
12 this is what this -- so you have this entity.
13 And it's a special entity because it's
14 designated in the code. The code designates
15 this special entity.

16 It's like, you know, there is a
17 special component in the system that has the
18 power to tell others what a UNL does in Ripple
19 code. It tells validators, listen to these
20 validators which are on this you list and,
21 basically, try to understand how many of those
22 validators are telling you something.

23 And if all -- not overwhelming, but a
24 large majority of these validators tells you
25 something, then do that. So now if you have the

1 [REDACTED] - Highly Confidential

2 power of the entity, which can serve this list
3 to validators, that's -- that's a -- that's a
4 large power. And the way the protocol was
5 designed, it requires trust into this part.

6 Q. Okay. In the context of an XRP -- of
7 the XRP Ledger, what is a Unique Node List?

8 A. The Unique Node List is the -- the
9 list of validators that validate the
10 transaction. So basically, they communicate
11 with the given validators. So each validator
12 has locally its own UNL, which is the list of
13 validators, that it considers. So as it accepts
14 messages from different validators, essentially,
15 it looks only the validators at its own UNL to
16 establish which ledger should be -- a ledger
17 means the block -- XRP Ledger should be added to
18 the blockchain.

19 Q. What did you do in this case to
20 research your understanding of a Unique Node
21 List?

22 A. I reviewed the code. I read the --
23 the Chase MacBrough paper. I made sure that my
24 understanding of rippled code matches the
25 explanations in Chase MacBrough paper. And I

1 [REDACTED] - Highly Confidential

2 looked at critical parts of the code, notably at
3 the quorum sizes, and -- basically how one
4 particular -- how particular parts of -- of the
5 protocol work. And this is what I did, yes.

6 Q. Okay. Let me direct you to page 6 of
7 your report.

8 A. Uh-huh.

9 Q. Under number two at the top of the
10 page, you write that Ripple controls the web
11 domain which hosts the service that provides the
12 dUNL to the XRP Ledger participants.

13 Correct?

14 A. Correct.

15 Q. What is the dUNL, as you use that term
16 in your report?

17 A. So the one item before that, so
18 page 6, Item 1, says, Participants required for
19 the proper operation of the system, in brackets,
20 nodes, are curated, under quotation marks, by
21 Ripple for inclusion into a specialist called
22 the dUNL, which is to be understood as default
23 Unique Node List.

24 So dUNL refers to the validators that
25 are included by Ripple in the special list that

1 [REDACTED] - Highly Confidential

2 is published from the validator list site, at
3 vl.ripple.com.

4 Q. Okay. Now, on page 6, you write that
5 your -- the statement that Ripple controls the
6 web domain which hosts the service that provides
7 the dUNL to XRP Ledger participants is true as
8 of the latest release of the XRP Ledger software
9 referred to as rippled Version 1.7.3. Right?

10 A. Uh-huh.

11 Yes.

12 Q. But, in fact, that's only true as you
13 note in number 3, For participants who use the
14 unmodified code of rippled Version 1.7.3.

15 Right?

16 A. Yes.

17 MR. SYLVESTER: Objection.

18 Q. You didn't consider any other version
19 of rippled other than Version 1.7.3 in reaching
20 the opinions in your report. Correct?

21 A. As we discussed, so there is -- you
22 need to fix the software in order to understand
23 what it does. So I was fixing the software to
24 default Version Ripple dot -- this 1.7.3.

25 Q. Okay.

1 [REDACTED] - Highly Confidential

2 Okay. Let me also direct you now to
3 the bottom of page 20 of your report.

4 And this is the paragraph just before
5 the bottom where you write that, quote, The
6 software fetches the latest published
7 recommended validator lists from the validator
8 list site at regular intervals.

9 Closed quote.

10 You see that?

11 A. Yes.

12 Q. For that statement, you rely on the
13 validator site .h file that's part ofrippled?

14 A. Yes.

15 Q. Okay. I'm going to show you now
16 what's marked as [REDACTED] 14.

17 (Report Citation was marked [REDACTED] Exhibit
18 14 for identification, as of this date.)

19 Q. Okay. My question to you is whether
20 you recognize this document.

21 MR. SYLVESTER: This has several
22 pages, so take your time to take a look at
23 it.

24 (Witness reviewing document.)

25 Q. Okay. Dr. [REDACTED] is Exhibit 14

1 [REDACTED] - Highly Confidential

2 the -- the same thing that you referred to in
3 your report as the citation for the sentence
4 that the software fetches the latest recommended
5 validator list?

6 A. It appears to be, yes.

7 Q. What role does the validator site .h
8 file play in the rippled code?

9 A. So as the comment says, This class
10 manages set of configured remote sites used to
11 fetch the latest published, recommended
12 validator lists.

13 Q. Where are you reading from?

14 A. Lines 43 and 44.

15 Q. Okay. Can you point to me the -- the
16 line of the code that you're looking at for that
17 portion of your opinion?

18 A. I'm looking at lines 43 and 44,
19 comments what the validators list -- validator
20 site does.

21 Q. Okay. And what role does line 46
22 play?

23 A. This is a comment.

24 Q. Also a comment.

25 Let me direct your attention to

1 [REDACTED] - Highly Confidential

2 line 24.

3 That code -- what is -- do you
4 understand what line 24 is?

5 A. It includes validator list .h into
6 this C file, yes.

7 Q. Did you review that file, validator
8 list .h, when preparing your report?

9 A. I do not recall for certain. I might
10 have. I might have not.

11 Q. Okay. Let me show it to you. It's
12 marked as Exhibit 15.

13 (Document was marked [REDACTED] Exhibit 15 for
14 identification, as of this date.)

15 Q. And you should, you know, please take
16 a moment to review it and let me know when
17 you're ready. I'll let you know that the
18 section that I'm going to direct your attention
19 to starts on line 375.

20 (Witness reviewing document.)

21 Q. Dr. [REDACTED] do you recall reviewing
22 this document in preparing your report?

23 A. I -- I think I saw this document.
24 Yes.

25 Q. When role does the ripple -- excuse

1 [REDACTED] - Highly Confidential

2 me. Let me rephrase.

3 What role does the validator list .h
4 file play in the rippled code?

5 A. I would need more time to tell you
6 exactly the answer to that question.

7 Q. Are you sure you've seen this document
8 before today --

9 A. I'm not sure.

10 Q. -- Exhibit --

11 A. I think I did. I cannot vouch I did.

12 Q. -- Exhibit 15?

13 A. Yes. I cannot vouch I did.

14 Q. Well, let me direct you specifically
15 to lines 375 and 376.

16 A. Yes.

17 Q. And those state, quote, Apply multiple
18 published lists of public keys, then broadcast
19 it to all peers that have not seen it or sent
20 it.

21 Closed quote.

22 Did you review these comment lines in
23 preparing your report?

24 MR. SYLVESTER: Objection. Asked and
25 answered.

1 [REDACTED] - Highly Confidential

2 Q. You can answer.

3 Dr. [REDACTED]

4 A. I don't -- I don't recall...

5 I don't recall evaluating these --

6 these particular lines of code.

7 Q. Okay. So you don't recall looking at
8 the comment lines in 375 and 376.

9 Correct?

10 A. Yes.

11 Q. Okay. So let me direct your attention
12 now to lines 404 through 413.

13 A. Uh-huh.

14 Q. Did you review those lines of code in
15 preparing your report?

16 MR. SYLVESTER: Objection.

17 A. I stated in my report which lines
18 of -- basically which lines of code I reviewed
19 in my report.

20 So --

21 Q. Where do you do that?

22 A. Basically, when I say, According to
23 this line and that line, basically, these are --
24 this is where I do it.

25 Q. Can you -- my question is, did you

1 [REDACTED] - Highly Confidential

2 review lines of code 404 through 413 of
3 Exhibit 15, in preparing your report?

4 A. I do not recall doing that.

5 Q. Did you -- did you review any part of
6 the rippled code other than the -- than the
7 portions expressly cited in your report?

8 A. I did.

9 Q. Okay. What do lines 404 through 413
10 of the code in Exhibit 15 mean?

11 A. To give you the full answer to that, I
12 would need to review this in more details.

13 Q. Do -- take a look at those lines of
14 code. Do they mean that the node will broadcast
15 its trusted Unique Node List to peers that have
16 not seen or sent it?

17 MR. SYLVESTER: Objection. Asked and
18 answered.

19 A. This particular code -- so this
20 particular signature doesn't say what happens.
21 It's just a signature of a function. So it
22 doesn't say what happens.

23 It's called in a certain way, but
24 implementation is missing.

25 Q. I'm sorry. I didn't follow that

1 [REDACTED] - Highly Confidential

2 answer.

3 A. The answer is, no, it does not.

4 Q. Your testimony is it doesn't mean that
5 the node will broadcast its trusted unique
6 node --

7 A. It has a signature -- it has a
8 signature of the function. It misses the
9 implementation of the function.

10 Q. Did you take this code into account in
11 forming your opinions in this case.

12 A. So this particular signature of the
13 function, I didn't take into account.

14 Q. Okay. So backing off from the code,
15 let's assume for a moment that the rippled code,
16 provides for peer-to-peer sharing of UNLs.

17 A. Uh-huh.

18 Q. First, do you know if that's true or
19 not?

20 A. I know that the -- the -- the -- the
21 UNLs are rebroadcasted. That I know. So if you
22 call this peer-to-peer sharing of UNLs, this is
23 possible, yes.

24 Q. Do you discuss that manner of sharing
25 UNLs in your -- anywhere in your report?

1 [REDACTED] - Highly Confidential

2 A. I do not.

3 Q. Why not?

4 A. It is not relevant to the need that
5 you trust -- need to trust this particular
6 issuer of the UNL.

7 Q. Why is peer-to-peer sharing with UNLs
8 irrelevant, in your view?

9 A. So what's the sharing going to
10 achieve? Is it going to achieve that we agree
11 on the same -- if it combines, even, the UNLs,
12 and sends it to all, there needs to be a
13 consensus protocol there, which make sure that
14 we look at the same view of a UNL. That's the
15 first thing.

16 The other thing I'm pointing out in my
17 report is that the UNLs need not to contain
18 malicious nodes. So you need to trust that the
19 UNL is sure even. If it doesn't serve different
20 UNLs to different nodes, you need to trust it
21 not to include malicious nodes.

22 Q. Okay.

23 A. So the trust in the UNL remains.

24 The -- my conclusion doesn't necessarily --
25 doesn't depend on the outcome of what the

1 [REDACTED] - Highly Confidential

2 mixing -- potential mixing of UNL is trying to
3 achieve.

4 Q. Let me focus back on the same sentence
5 in paragraph -- on page 20, where you cite --
6 you stated that the software fetches the latest
7 published, recommended validator list from the
8 validator list site at regular intervals.

9 A. Yes.

10 Q. If the rippled code provides for
11 peer-to-peer sharing of UNLs, would you agree
12 that that's another way that nodes might receive
13 an updated UNL that does not require loading the
14 validator list site?

15 MR. SYLVESTER: Objection.

16 A. So the -- the source of the file
17 remains the same. You can get it directly from
18 the source or not. It is authenticated by the
19 source, and the source remains the same. So if
20 you get it from somebody else, you're getting
21 the same information, that this validator list
22 site published.

23 Q. Okay. Can you -- I want to know if
24 you're able to answer this question yes or no.

25 Can you answer yes or no: Would

1 [REDACTED] - Highly Confidential

2 peer-to-peer sharing be another way that nodes
3 might receive an updated UNL that does not
4 require loading the validator list site?

5 A. It might be another way to do that.
6 Yes.

7 Q. Okay.

8 A. It's a -- yeah. It's also not very --
9 not necessarily a reliable way, but it's one way
10 to do it, yes.

11 Q. Okay. In -- in -- in preparing your
12 report in this case, did you consider the impact
13 of peer-to-peer sharing of UNLs on your
14 opinions?

15 MR. SYLVESTER: Objection.

16 A. What I considered in my -- in my
17 report, I presented it. And yes. So --

18 Q. Well, I'm not sure I understand what
19 you're saying yes to. Earlier you acknowledged
20 that your report does not address peer-to-peer
21 sharing. Correct?

22 A. Yes -- well, I was aware that
23 validators, if they download the list, they can
24 forward it to other nodes.

25 Q. Did you consider the impact of

1 [REDACTED] - Highly Confidential

2 peer-to-peer sharing of UNLs on the opinions
3 that you've included in your report?

4 MR. SYLVESTER: Objection.

5 A. I mentioned it, so I was aware that
6 this is happening. And, again, this -- to my
7 understanding of the system, it doesn't impact
8 my conclusions.

9 Q. So does the operation of peer-to-peer
10 sharing of UNLs affect your contention that if a
11 corrupted dUNL publisher served totally
12 different UNLs to different validators, that
13 would prevent the correct operation of the
14 XRP Ledger?

15 A. If it happens, and you have a protocol
16 that exchanges the UNLs among nodes, you will
17 still need to prove that the UNLs exchanged --
18 actually, somehow magically combines into the
19 same UNL. Because with the -- without
20 sufficient overlap, and there is no point in the
21 code that suggests that.

22 Q. But that -- you're talking now --
23 you're talking about other conditions that might
24 need to be met. I'm -- I'm just restricting
25 myself to the -- your opinion that you share on

1 [REDACTED] - Highly Confidential

2 page 22 that -- where you wrote that if a
3 corrupted dUNL publisher -- a corrupt -- I'm
4 sorry. Let me make sure you're -- let me direct
5 your attention to page 22 in the middle.

6 Do you see your sentence where you
7 write, quote, As a simple example, a corrupted
8 dUNL publisher may serve totally different UNLs,
9 i.e., 0 percent intersection, to different
10 validators, preventing the corrupt -- the
11 correct operation of the ledger.

12 Do you see that?

13 A. I see that.

14 Q. Does the operation of peer-to-peer
15 sharing of UNLs affect that contention?

16 A. It does not, because the -- still, the
17 publisher can serve different UNLs to different
18 validators without the necessary intersection
19 among the UNLs. So my sentence would stay as
20 it's written.

21 Q. Okay. If the publisher did that,
22 served a corrupted -- hold on. Restate.

23 If the publisher did that, would
24 peer-to-peer sharing render that action
25 ineffective?

1 [REDACTED] - Highly Confidential

2 MR. SYLVESTER: Objection.

3 A. How do you define "ineffective"?

4 Q. Could the ledger still make forward
5 progress and operate?

6 MR. SYLVESTER: Objection.

7 A. Yeah. To my -- to my best
8 understanding, it would not.

9 Q. It would not operate.

10 A. It would -- it would be possible that
11 it -- that it does not operate. It would not
12 guarantee that the problem is fixed.

13 Q. Could it still operate? I'm trying to
14 understand. Are you saying that, if there's a
15 corrupted dUNL publisher, even if UNLs are
16 shared through peer to peer, that's it; the
17 ledger would stop operating?

18 A. So when you say "could," even if there
19 is no peer-to-peer sharing, even if there is --
20 Byzantine dUNL publisher serving lists to
21 different nodes, completely different validator
22 lists, and they operate on validator lists,
23 there is a possibility that the ledger continues
24 even though. So basically this is where you
25 agree on the same -- on the -- on the -- on the

1 [REDACTED] - Highly Confidential

2 same information.

3 Q. Okay. So it's still -- there is still
4 a possibility, that the ledger could continue to
5 function.

6 MR. SYLVESTER: Objection.

7 A. There is always possibility that it
8 would. There is possibility that it wouldn't.

9 Q. Okay. So if there's a corrupted dUNL
10 publisher, your position is that it's possible
11 the ledger could continue to function, or it's
12 possible that it wouldn't?

13 A. It's probable that it wouldn't.

14 Q. You're not saying that for a hundred
15 percent, correct?

16 A. I'm not saying --

17 MR. SYLVESTER: Objection.

18 A. To my understanding of the -- of the
19 opinion, I would need more time to understand
20 it.

21 Q. Okay.

22 A. Is it 100 percent that it stops, or is
23 it just probable that it stops.

24 Q. Why would you need more time? Why did
25 your work on the case to date not sufficiently

1 [REDACTED] - Highly Confidential

2 allow you to answer that question with a
3 definitive answer yes or no?

4 MR. SYLVESTER: Objection.

5 A. I did this work three months ago. So
6 I spent the time I spent. It's a complex system
7 which has different properties to it. And I
8 don't necessarily recall all what I learned then
9 about the system. Unfortunately, my
10 understanding of the system today is not at
11 the -- as detailed level as I understood then.
12 That would be the best answer I could give.

13 Q. Okay. All right. Turning to a
14 different subject.

15 Is it -- I think we've talked about
16 this, but I just want to make sure. Is it
17 possible, in your view, that a blockchain system
18 could start out as centralized and become
19 decentralized over time, with changes?

20 A. I believe this is possible.

21 Q. Are you aware of any accepted
22 scientific tests for determining the moment in
23 time when a blockchain system goes from
24 centralized to decentralized?

25 MR. SYLVESTER: Objection.

1 [REDACTED] - Highly Confidential

2 A. If we adopt the approach that I'm
3 suggesting, with my approach, so basically that
4 in each point of time when software changes and
5 the circumstances changes, you validate a
6 system. Then if you applied this fine
7 granularity, you could come to the point where
8 it happens. It could go back and forth
9 probably. It could be decentralized and
10 centralized again and so on.

11 Q. But my question is if you're aware --
12 I understand we'll talk about your methodology
13 that you've proposed here. But are you aware of
14 any generally accepted scientific test for
15 determining that moment in time when a
16 blockchain system goes from centralized to
17 decentralized or decentralized to centralized?

18 A. So many in the bitcoin and material
19 world, many papers talk about, for example,
20 centralization in the mining pools. So that's a
21 fairly subjective -- subjective -- maybe
22 debatable assumption, because it's -- it
23 assumes, so that assumption assumes that the
24 mining pool operator controls all the nodes in
25 the mining pool.

1 [REDACTED] - Highly Confidential

2 And then -- so some authors analyze
3 the mining power concentration in bitcoin and
4 Ethereum. And they would say this many mining
5 pools, if they come together and combine their
6 hash power, they would go over 51 percent.

7 And at that point, I saw some
8 basically -- you know, I'm pretty -- I'm aware
9 that there is some analysis, at which points
10 this number shrinks, for example, from four
11 mining pools to three mining pools to five
12 mining pools and maybe to one mining pool. And
13 at that point of time, blockchain system could
14 be so.

15 There is a reason to call it
16 centralized, because there is still not --
17 again, coming back to our probability versus
18 possibility, it's possible. But let's say if
19 it's possible that the violation happens, if
20 you're conservative, you would assume that it
21 could actually happen.

22 Q. Okay. You were just talking about
23 concentration in mining pools, correct?

24 A. Yes.

25 Q. Would you agree that's one aspect of a

1 [REDACTED] - Highly Confidential

2 decentralized system?

3 Or let me -- that's one -- one aspect
4 to consider, of whether a blockchain system is
5 decentralized?

6 A. The consensus protocol is the most
7 important one. So in the Sai paper that you --
8 that you submitted as Exhibit [REDACTED] 4, Sai actually
9 for the different aspects of decentralization,
10 they perform the interview with the experts.
11 Like, do you believe -- asking them, Okay, we
12 have these different aspects of
13 decentralization, and do you believe this is
14 relevant or not.

15 So if you look at --

16 Q. I'm going to -- I'm going to --

17 A. Yes.

18 Q. I don't think you're answering my
19 question, so I want to rephrase it. And I want
20 to try to ask you to focus on the questions that
21 I'm asking.

22 A. Uh-huh.

23 Q. So, first of all, one question I
24 asked, was, are you aware of any scientific test
25 for determining the moment in time when a

1 [REDACTED] - Highly Confidential

2 blockchain system goes from centralized to
3 decentralized?

4 MR. SYLVESTER: Objection.

5 A. I believe I described you such a
6 moment. It's the moment -- for example, in the
7 case of proof-of-work mining pools, it's the
8 moment where the one mining pool goes beyond
9 51 percent of power. I tried this convey this
10 is one possible test. So I'm aware of such a
11 scientific, accepted test that you can verify.

12 Q. So in the comparison you just gave
13 with a 51 percent attack, isn't that example of
14 a system going from centralized to -- from
15 decentralized to centralized?

16 A. It's the same the other way around.
17 If you go from -- if you had a snapshot in time
18 where one -- one mining pool controlled
19 51 percent of power and you go to the world
20 where two mining pools actually have it or more,
21 you would go from centralization to
22 decentralization.

23 Q. Outside of proof-of-work consensus
24 protocols, are you aware of any accepted test
25 for determining the moment when a blockchain

1 [REDACTED] - Highly Confidential

2 system goes from centralized to decentralized?

3 A. I would say this is the moment where a
4 system passes Troncoso test.

5 Q. And is the Troncoso test the accepted
6 scientific test?

7 A. I would say, if we -- so we argue --
8 we discussed this for one hour before. So we
9 discuss the minimality of the Troncoso
10 definition.

11 And, what do you mean by "accepted"?
12 So accepted by whom?

13 Q. Well, as of October 6, 2021, you --
14 you spoke about there being no consensus until
15 you saw the Troncoso test.

16 A. I'm speaking --

17 MR. SYLVESTER: Objection.

18 A. I'm speaking about past.

19 Q. Okay. Do you think that the whole
20 scientific community has accepted the Troncoso
21 test as the accepted test for determining the
22 moment when a blockchain system is
23 decentralized?

24 A. I will repeat again what I said
25 before. So, I'm not aware of any definition of

1 [REDACTED] - Highly Confidential

2 decentralization that would go against Troncoso
3 definition and that would still call the system
4 decentralized.

5 If you ask me that question, I can
6 only repeat what I said before, is that I think
7 there is a consensus on this minimal and
8 necessary definition.

9 Q. Okay.

10 All right. I'm going to show you
11 another exhibit, Exhibit 5.

12 (Position paper [REDACTED]
[REDACTED] was marked [REDACTED]

14 Exhibit 5 for identification, as of this
15 date.)

16 Q. Do you recognize this document?

17 A. I do.

18 Q. What is it?

19 A. This is my invited paper [REDACTED]
[REDACTED] peer

21 reviewed by [REDACTED]
[REDACTED], editor of the

23 [REDACTED]
[REDACTED]
[REDACTED], journal to which this paper

1 [REDACTED] - Highly Confidential

2 was invited.

3 My invitation was done by
4 [REDACTED], who is another editor
5 of the journal. They invited me to give my
6 opinion on decentralized computing as an expert
7 in the field.

8 Q. Okay. Now, is Exhibit 5 what -- the
9 same article that you cite to in your references
10 in your report as Reference Number 22?

11 A. Yes, it is.

12 I believe it is, so I should look at
13 all pages, but it appears to be, yes.

14 Q. At the time that you issued your
15 report in this case on October 4, 2021, had this
16 paper, Exhibit 5, been published yet?

17 A. It was accepted by the -- by the
18 reviewers, which are the editors of the -- of
19 the journal, which is why I cite it as -- under
20 the name of [REDACTED]

[REDACTED]. So at that
22 very moment it was peer reviewed, and it was
23 pending publication; it was in the process of
24 publication.

25 And I made it available on my website

1 [REDACTED] - Highly Confidential

2 as a preprint, which we usually do when -- when
3 we have this like small window between
4 acceptance and publication, this is what we do.

5 Q. Okay. I'm going to refer to
6 Exhibit 5, using your term, position paper. I'm
7 going to refer to it as your position paper.

8 A. Uh-huh.

9 Q. Is it -- is it your understanding that
10 the [REDACTED] is an academic journal?

11 A. Yes, it is.

12 Q. Okay. Is it -- does it represent
13 itself, as a peer-reviewed publication?

14 A. This is a peer-reviewed publication.
15 There are contributed publications -- I believe
16 there are contributed publications which are not
17 peer-reviewed. And this one is.

18 Q. When you're saying "this one is," you
19 mean your article was peer-reviewed?

20 A. My article is, yes.

21 Q. And specifically it was peer-reviewed
22 by [REDACTED]?

23 A. Professor [REDACTED], alumnus of [REDACTED]
24 and professor at [REDACTED]
[REDACTED]

1 [REDACTED] - Highly Confidential

2 Q. Did anyone besides [REDACTED] peer
3 review this paper?

4 A. So I know it was read, although no
5 particular feedback was provided, except as
6 high-level comments by [REDACTED], another
7 editor, Professor [REDACTED]
[REDACTED], who is another editor of
9 the journal.

10 Q. Okay. Were you the only author of
11 your position paper?

12 A. I am.

13 Q. So, when your position paper uses the
14 term "we," is that a writing convention, the
15 royal we, and you're really referring to I,
16 meaning yourself?

17 A. Yes, this is -- this is normal, and it
18 basically downplays your ego, and that's an
19 accepted approach in scientific writing. You
20 don't want to bother the reviewer by saying I,
21 I, I, I, and it feels better that -- at least
22 the way I was educated as a scientist, to write
23 we. That's a common -- commonplace.

24 Q. Okay. Let me direct your attention to
25 page [REDACTED] of Exhibit 5.

1 [REDACTED] - Highly Confidential

2 In the abstract --

3 A. Yes.

4 Q. -- at the top.

5 Do you see in the second paragraph,
6 you wrote, quote, [REDACTED]

9 A. I do.

10 Q. Okay.

11 So, as of [REDACTED], were you
12 acknowledging in this position paper that there
13 are existing definitions, plural, for
14 decentralized systems?

15 MR. SYLVESTER: Objection.

16 A. I do not.

17 Q. What did you mean by [REDACTED]
[REDACTED]?

19 A. So, we start by releasing the
20 definition of decentralized systems, briefly
21 surveying the literature on taxonomy and
22 different facets --

23 Q. Really, you may have to slow down for
24 the court reporter.

25 THE COURT REPORTER: I would

1 [REDACTED] - Highly Confidential

2 appreciate that. Yes.

3 THE WITNESS: Sorry.

4 A. Second paragraph, page

[REDACTED]

17 Q. So, are you saying that when you

18 wrote, [REDACTED], you

19 didn't mean existing definitions of

20 decentralized systems?

21 A. Concretely including this complements

22 the definition -- the distinction between

23 permissionless and permission systems.

24 As we discussed today, I believe, and

25 the methodology that I adopt supports, that both

1 [REDACTED] - Highly Confidential

2 permission and permissionless system can be
3 decentralized.

4 So what this particular inclusiveness
5 does, it -- you know, what I say in the paper
6 is -- and also in the report -- are
7 permissionless system truly permissionless? Or
8 they basically allow certain players to join the
9 game in a special role? Or are -- they are
10 permissionless in the sense they don't
11 require -- basically they give equal
12 opportunities, which is the same term, the --
13 the -- the term that I use for inclusiveness.

14 Q. Okay.

15 A. And in which case they would be called
16 truly permissionless.

17 Q. So --

18 A. So that's my attempt and contribution
19 to the -- contribution to discern -- for
20 example, it's very important if you discern
21 proof-of-stake and proof-of-work systems.

22 It's applicable -- this -- this report
23 doesn't write about XRP Ledger, but, for
24 example, if you have a system such as XRP Ledger
25 in which certain nodes are preferred, for

1 [REDACTED] - Highly Confidential

2 example, by their inclusion into the UNL,
3 they're more preferred than others, it allows
4 you to discern these categories.

5 Q. So, is inclusiveness about the degree
6 of permission rather than about the degree of
7 centralization?

8 A. I can give you the definition of
9 inclusiveness.

10 Shall I read it out for you or --

11 Q. No. Just tell me the page number
12 you're referring to.

13 A. [REDACTED]

14 Q. Okay. We can come back to that later.
15 I want to first direct you to page [REDACTED]

16 A. Uh-huh.

17 Q. In the first full paragraph, at the
18 top. You refer to, quote, [REDACTED]

[REDACTED], close quote.

20 What did you mean by that?

21 A. I meant -- let me just -- let me read
22 it. Sorry.

23 (Witness reviewing document.)

24 Where -- which line do you have that?

25 Q. It's the first full paragraph on the

1 [REDACTED] - Highly Confidential

2 top of page [REDACTED] And you write at the -- in the
3 last sentence, quote, [REDACTED]

[REDACTED] -- I'm sorry, the -- right before
5 that.

6 You write, [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

10 Do you see that?

11 A. Yes.

12 Q. What did you mean by [REDACTED]
[REDACTED]?

14 A. So these are the -- this is what is
15 explained in the following sentence. So, the
16 following sentence is actually describing in
17 more details what the sentence that you read out
18 does. So, I can read it out, we can discuss it.

19 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

23 So, flavors should be related to
24 definition of Troncoso and different facets.

25 Q. Okay.

1 [REDACTED] - Highly Confidential

2 All right. Let's turn to page [REDACTED] at
3 the bottom, where your [REDACTED] position
4 paper proposes [REDACTED]

[REDACTED] of inclusiveness, and argues that
6 inclusiveness should be added as a key property
7 of decentralized systems.

8 MR. SYLVESTER: Can -- can you point
9 us to [REDACTED] please?

10 MS. ZORNBERG: It's on page [REDACTED]
11 actually. The use of that language.

12 At the -- the paragraph at the -- in
13 the middle of the -- the paragraph at the
14 top, you wrote, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

19 Do you see that?

20 A. I see that.

21 Q. Okay. So do you agree that your [REDACTED]
22 position paper [REDACTED]

[REDACTED]

24 A. I agree.

25 Q. Were you the first to make that

1 [REDACTED] - Highly Confidential

2 proposal?

3 A. I was.

4 I am.

5 Q. Okay. And you felt that you were
6 making a contribution to the scientific
7 community by -- by making that proposal --

8 A. I do.

9 Q. -- correct?

10 A. I still do. I did, and I do.

11 Q. Okay.

12 And you provide a -- a definition of
13 inclusiveness on page [REDACTED] and you provide a
14 definition of equal opportunities, which is part
15 of your definition of inclusiveness, at the

16 [REDACTED]

17 Right?

18 A. Yes.

19 MR. SYLVESTER: Take your time if you
20 need a second to read it.

21 A. So Definition 2, inclusiveness, says
22 that basically it's -- you can consider it
23 renaming. So the system is including if and
24 only if it satisfies equal opportunities, and
25 equal opportunities is then defined in

1 [REDACTED] - Highly Confidential

2 Definition 1.

3 Q. Okay. Can a -- can a system be
4 decentralized but not inclusive?

5 A. It could. According to Troncoso
6 definition, it could, and we discuss. So
7 permission systems, we already admitted in the
8 earlier part of this deposition that permission
9 systems can be decentralized.

10 And clearly, if you -- if you read
11 this, you will see that permission systems are
12 not inclusive, which answers your question.

13 So it's not a necessary requirement.

14 Q. It's not -- inclusiveness is not a
15 necessary requirement for --

16 A. It's --

17 Q. -- decentralization --

18 A. According to --

19 MR. SYLVESTER: Let her finish the
20 question, please.

21 THE WITNESS: Sorry. Sorry.

22 Q. So just to rephrase, so do I
23 understand you to be saying that inclusiveness
24 is not a necessary requirement to
25 decentralization; rather, a decentralized system

1 [REDACTED] - Highly Confidential

2 can be inclusive or not inclusive?

3 A. You got it right.

4 Q. Okay.

5 That will -- that's at least one
6 thing. At least one thing.

7 A. No, you got many things right.

8 Q. Okay.

9 So, let's focus on your definition of
10 equal opportunities, at the bottom of [REDACTED],
11 [REDACTED]. Did you come up with that
12 definition?

13 A. I did.

14 Q. Okay. And is that also a new
15 definition that you put out into the scientific
16 community?

17 A. As you see --

18 MR. SYLVESTER: Objection.

19 Go ahead.

20 A. As you see, we already discussed this,
21 and yes, this is one of the -- in the abstract,
22 I even say we complement. In abstract, you
23 typically say what you did in the paper, and I'm
24 proposing including this, and I'm arguing it's a
25 critical facet, so that's a new contribution

1 [REDACTED] - Highly Confidential

2 to -- that's a new contribution, you -- you are
3 right, yes.

4 Q. Okay. To date, do you know whether
5 your definition of equal opportunities has been
6 adopted by the scientific community?

7 A. We need to define "adopted." I will
8 say, you know, adoption in a sense that people
9 cite this work, and it has been a month or two.
10 So I gave a few talks about it, so I talk about
11 this, in the video that you -- that you played,
12 during [REDACTED]

13 I gave already two invited lectures on
14 the topic. So, at the red chain workshop which
15 is organized by the [REDACTED]

[REDACTED], I was invited to give a talk where I
17 presented the concept.

18 And, let's say, so I -- it's not
19 adopted yet but, you know, these things takes
20 time. So nobody opposed it, nobody says, This
21 is nonsense or anything. So far so good.

22 Q. To your knowledge?

23 A. Yes, to -- nobody told -- well, nobody
24 told me, yes, so if there is -- yeah, let's
25 speak in the open so...

1 [REDACTED] - Highly Confidential

2 And then the next lecture where I
3 mentioned it is the -- I gave the lecture just
4 this Monday on [REDACTED] so my alma
5 mater, basically, where I did Ph.D., I was
6 invited to give a lecture on decentralized
7 computing, and there, I mention to the students
8 this definition.

9 Q. Okay. Have you checked Google Scholar
10 to see whether your position paper has received
11 any citations to date?

12 A. I checked maybe last week. And in
13 this one month or so, it didn't yet.
14 To my knowledge.

15 Q. Okay.

16 I'll represent we checked this morning
17 and saw no -- no listed citations to your
18 position paper.

19 A. It takes time.

20 Q. It takes time?

21 A. If you may add, may I add something?
22 Or not?

23 Q. If it's -- if it's brief, sure.

24 A. Troncoso paper has like more citations
25 than -- than others that came up into this --

1 [REDACTED] - Highly Confidential

2 so, you know, if you're measuring this -- if
3 you're measuring the impact of the paper, for
4 example, it's not a fair measure because Sai
5 paper came in 2021 and Troncoso in 2017, but
6 there is a considerable -- considerably more
7 citations for Troncoso paper than other papers
8 we mentioned today.

9 Q. Okay. When did you draft your
10 position paper, Exhibit 5, in relation to your
11 work on this case?

12 A. So --

13 MR. SYLVESTER: Objection. Go ahead.

14 A. Yes. So, I need to recall precisely.
15 The concepts -- for example, the concept of
16 inclusiveness, I got before I was contacted with
17 [REDACTED] I'm not sure I called it my head
18 inclusiveness.

19 But this distinction about specialized
20 players in the system, for example, let's --
21 let's not bash XRP Ledger too much. Let's talk
22 about proof of stake and proof of work.

23 So this distinction between the two
24 that was trying to capture the essence of
25 inclusiveness, that -- that was born early this

1 [REDACTED] - Highly Confidential

2 year. So before --

3 Q. Early 2021 --

4 A. Early 2021.

5 Q. -- you started thinking about
6 inclusiveness?

7 A. Yes. I -- I started to -- I was
8 trying -- for example, in proof-of-stake and
9 proof-of-work comparison, I was trying to
10 capture in my head, what's the difference. They
11 appear permissionless to -- to anyone, but there
12 is a difference, and it's not in these attacks.

13 So in the first hour of my deposition
14 I talked about attacks and proof of stake and
15 how you checkpoint in proof of work. So it's
16 not about that. So here is more fundamental
17 distinction.

18 So that was born before -- that was
19 born before I was invited to write this position
20 paper and before I was contacted by [REDACTED]

21 The writing that you asked me --

22 Q. Would you --

23 A. Yeah.

24 Q. I'm sorry, were you finished with your
25 answer?

1 [REDACTED] - Highly Confidential

2 A. Yeah, I am.

3 Q. Okay. Would you agree that there's --
4 there's overlapping content between material in
5 your report in this case and the material in
6 your position paper?

7 A. I do.

8 Q. Okay. What about the -- the
9 four aspects of a decentralized system in your
10 report, in this case; you also cite to the same
11 aspects in your position paper, correct?

12 A. Yes, I do.

13 Q. Okay. So which did you -- which did
14 you -- did -- did you devise that methodology
15 first for your work on this case, and then
16 incorporate it into your paper, or did you
17 devise it for the paper and then use it in this
18 case?

19 A. So --

20 MR. SYLVESTER: Objection.

21 Go ahead.

22 A. Yes. So, I don't recall
23 necessarily -- so -- I would say I was
24 interested in defining decentralization. I was
25 invited to write this position paper before I

1 [REDACTED] - Highly Confidential

2 started working on this case.

3 So the invitation came in --
4 definitely in the first -- before May this year,
5 maybe a bit earlier.

6 I think it's -- it's earlier because
7 I -- I was -- I was supposed to write something
8 for the May edition. Yes. It was earlier. So
9 I was supposed to not go for the October issue,
10 but I was supposed to go for the May issue in
11 the beginning, and then I postponed it because I
12 was [REDACTED], et cetera, but I was supposed
13 to write an article. So that invitation for the
14 position came -- paper came before this work.

15 Then when I was reviewing the
16 literature to -- in the -- for the context of
17 this case, when you asked whether the system is
18 decentralized or not, I realized, okay, you are
19 invited -- your invited contribution should be
20 on decentralized systems. This is how -- this
21 is how it came to me, presented by editors.

22 But, you know, if you say
23 "decentralized systems," you better include the
24 definitions so the readers know what you're --
25 what you're talking about.

1 [REDACTED] - Highly Confidential

2 Since I was already looking into
3 this -- of the case, I thought, Okay, why not --
4 you know, no mention -- as you see, no mention
5 of the case or anything. Why not share this
6 work with others.

7 And there are other contributions of
8 the paper, so it's not -- it's not
9 double-spending the report and publishing it, so
10 there is additional things in the paper.

11 Q. Okay. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Was that coincidence?

15 A. It was -- it was accepted just
16 recently. So it -- it's really like you see,
17 the -- the date were like fitting in the same.
18 We can call it a coincidence. I mean, so yes.

19 Q. To your knowledge --

20 A. It could -- it could go like -- you
21 know, if the -- if the invitation -- if the --
22 if the paper was supposed to publish -- be
23 published in November, I couldn't have -- not
24 have done it.

25 And if -- I didn't think, but I was

1 [REDACTED] - Highly Confidential

2 supposed to submit my report in September, and
3 then I didn't, and then I submitted it in
4 October, so we can call it a coincidence.

5 Q. Okay. To your knowledge, was the SEC
6 aware of your draft position paper?

7 A. Did -- did SEC review my paper or
8 something?

9 Q. Well, did -- to your knowledge, did
10 the SEC know that you were publishing this
11 position paper?

12 A. I -- I advised -- I'm not sure I talk
13 to SEC. I advised [REDACTED] that I'm going to use
14 part of the methodology to -- for the paper.
15 And I basically made that known.

16 Whether SEC knew it or just [REDACTED]
17 knew it, I definitely made it clear, yes.

18 Q. Okay.

19 Did anyone from the SEC or [REDACTED]
20 provide comments on your draft position paper?

21 A. No, they did not.

22 Q. Okay.

23 Turning to another subject.

24 Do you degree that there are different
25 architectural layers within blockchain systems?

1 [REDACTED] - Highly Confidential

2 A. Within a softwares -- within a
3 software system, computer system, there are
4 different layers. Including -- if the
5 blockchain is a computer system, there are
6 different layers to the blockchain system as
7 well.

8 Q. Okay. So if you still have Exhibit 4
9 in front of you, the Sai paper --

10 A. Yes.

11 Q. -- let me ask you to turn to page 12.

12 Do you see the chart that he has --
13 that Sai labels as Table 2?

14 A. I see.

15 Q. Okay. And in the left column of the
16 chart, do you see that Sai identifies -- it
17 looks like six different layers of -- within
18 public blockchains.

19 A. I see it.

20 Q. Do you -- do you think that Sai has
21 omitted any layers? In other words, are there
22 additional layers of public blockchains not
23 identified here?

24 A. That's a good question.

25 So, I think he covered them well.

1 [REDACTED] - Highly Confidential

2 Let's look excluded, there is, you
3 know, something, but I think it's -- covers it
4 well but -- you know.

5 Q. Okay. And in the -- in the next
6 column, middle column, Sai identifies what he
7 calls different factors of centralization within
8 each layer of a blockchain, of a public
9 blockchain system.

10 Do you see that?

11 A. Where do you find that?

12 Q. The middle column.

13 A. Centralization factor.

14 Q. So, for example, for the network
15 layer, do you see that Sai identifies
16 four distinct centralization factors to
17 consider, just within the network layer?

18 MR. SYLVESTER: Objection.

19 A. I see that there is a "Network Layer"
20 row. I see that there is a "Centralization
21 Factor" column. I see that there are
22 four different centralization factors in the
23 "Network Layer" row.

24 Q. Do you agree with Sai that aspects of
25 centralization at the network layer are relevant

1 [REDACTED] - Highly Confidential

2 to overall assessment of decentralization of
3 blockchain systems?

4 MR. SYLVESTER: Objection.

5 A. I do. So I agree that the network
6 layer centralization is important for evaluating
7 whether the entire software system, distributed
8 software system including blockchain, is
9 centralize -- is decentralized or centralized or
10 not.

11 Q. Do you agree that each different
12 factor of centralization within an application
13 layer may require a different measurement
14 technique?

15 MR. SYLVESTER: Objection.

16 A. Can you repeat that again? I
17 apologize.

18 Q. Yeah.

19 So, do you see how in -- in Sai's
20 chart, Table 2, Sai also has a column on the
21 right called "Measurement Techniques," where Sai
22 lists different techniques for measuring each
23 centralization factor within each layer of a
24 public blockchain?

25 A. I see that.

1 [REDACTED] - Highly Confidential

2 Q. Do you agree that the scientific
3 community may need to use a different
4 measurement technique in order to measure
5 different centralization factors?

6 MR. SYLVESTER: Objection.

7 A. What I think is that scientific
8 community could use those, it could use some
9 others. It's like what -- what are you
10 measuring, doesn't necessarily -- is important.
11 And then comparing what you're measuring doesn't
12 necessarily depend on the metric you're using.

13 I can give an example. So, I can
14 measure the height of people by a yardstick, or
15 by a meter, or by a foot.

16 So these are different, you know,
17 measurements, and they might come up to the same
18 conclusions. In my example they would, but
19 which person is taller than other, which -- in
20 other cases, you know, some conclusions might be
21 different.

22 So does this help?

23 Q. Well, I want to just make sure I
24 clarify. Would you agree then that even today,
25 there's ongoing dialogue in the scientific

1 [REDACTED] - Highly Confidential

2 community about which metrics to use in
3 measuring different aspects of decentralization?

4 A. I would say which metrics you use, but
5 not what are you measuring. So that's important
6 distinction.

7 So, for example, geographic
8 distribution, so, you know, if you're measuring
9 geographic distribution, you would go and
10 measure it something.

11 And then you can use what he says,
12 Gini coefficient and latency, which is like, you
13 know, just reading this, Gini coefficient of
14 what? You need to say of what? Right? And
15 things like that so that's a bit imprecise.

16 But yes, I mean, you can use different
17 metrics. I would say it's more important to
18 focus what are you measuring.

19 Q. Okay. In your report, did you
20 consider centralization aspects for every
21 blockchain layer?

22 A. So, you will see that my methodology
23 points -- so focuses, and points out, resilience
24 layer, which is essentially consensus layer. It
25 maps to the consensus layer of Sai. If you want

1 [REDACTED] - Highly Confidential

2 to do the mapping, it maps to the -- maps to the
3 consensus layer.

4 Then there is the openness layer. Ah,
5 so you see, okay, openness that I discuss in my
6 report, it's -- so Sai focuses on public
7 blockchain systems. And then if you want -- so
8 as the title says, "Taxonomy of Centralization
9 in Public Blockchain Systems."

10 Then he goes -- they go and compare to
11 bitcoin and Ethereum -- compare bitcoin to
12 Ethereum, and this is their focus.

13 So, for example, they wouldn't -- this
14 doesn't discuss permission blockchains, whether
15 they can be centralized or not, so there is a
16 point of contention maybe there, but, again,
17 Troncoso definition would allow permission
18 blockchains.

19 So you asked me before, and then I
20 will need to complement, is there a layer that
21 Sai doesn't consider? And that would be this
22 openness --

23 Q. Okay.

24 A. -- layer that I'm considering.

25 Q. So let me just break it down. First I

1 [REDACTED] - Highly Confidential

2 hear you saying that one layer, not referenced
3 in Table 2 of Sai, that you think is important
4 to evaluating decentralization, is openness?

5 MR. SYLVESTER: Objection.

6 A. That's -- it's not that I think it
7 is -- it is important, it's that also I think
8 that it is important, and there are other people
9 who think that it is important to look whether
10 it's -- blockchain is permissioned or not, when
11 we evaluate which one is more decentralized than
12 the other.

13 So if I'm to point out the layer that
14 not only me but also other researchers and other
15 just -- whoever works in this space -- considers
16 as an important aspect or facet of
17 centralization, decentralization, is the
18 openness.

19 This is related to permissionless,
20 permissionness and inclusiveness that we
21 discussed in this deposition.

22 Q. Okay.

23 Do you degree that your report, in
24 evaluating and comparing blockchain systems, did
25 not analyze every single layer that Sai lists in

1 [REDACTED] - Highly Confidential

2 Table 2?

3 A. In my report, I mention all the layers
4 that Sai discusses.

5 And notably, you know, with respect to
6 network and application layer, these are
7 mentioned in my report in -- sorry, just a
8 second. I got lost.

9 Q. Are you talking about page 11?

10 A. Maybe.

11 Yes.

12 Q. Okay.

13 A. So, for example, in the network layer
14 I mentions -- I can read it out -- but some
15 authors -- I'm citing Sai -- consider additional
16 aspects of decentralization including
17 decentralization of the net --

18 THE COURT REPORTER: Slow down a
19 little for me.

20 MR. SYLVESTER: Yes.

21 THE WITNESS: Sorry about that.

22 A. Finally, I'm reading out the --
23 page 11.

24 Q. You don't have to read it out loud.

25 But I --

1 [REDACTED] - Highly Confidential

2 A. Okay.

3 Q. I'm on the same page. You're --
4 you're referring to the paragraph in the middle
5 of page 11 --

6 A. Yes.

7 Q. -- just above 3.2 of your report?

8 A. Yes.

9 Q. Is it fair to say that you -- this is
10 the part of your report where you identify that
11 some authors have considered aspects of
12 decentralization that you are not focusing on in
13 your methodology?

14 A. Focusing is the right word, although I
15 say -- and I would definitely like to read this
16 out -- decentralization at the network layer
17 requires that no single authority can control
18 all the participants of a decentralized system
19 at the network and infrastructure layers.

20 So I'm pointing it out, and then I'm
21 focusing -- in the next paragraph, I'm saying we
22 are going to focus on these other aspects, which
23 don't touch the network layer.

24 I can give you -- if you wish, I can
25 give the justification, which is not included in

1 [REDACTED] - Highly Confidential

2 the report, my line of thinking, why this was
3 the --

4 Q. Please do.

5 A. Great. Thank you.

6 So, all of three compared systems.
7 They operate on wide area Internet.

8 Q. On?

9 A. On wide area internet.

10 So bitcoin, Ethereum and XRP Ledger.

11 In my opinion, there is no
12 centralization at the network layer for either
13 of the three.

14 And then I -- they're like more -- I'm
15 not saying there are no differences. Of course,
16 if you look at the network distribution of all
17 three blockchains, it's actually very different,
18 and we can discuss that in a moment.

19 The main difference is that XRP Ledger
20 has much fewer nodes than bitcoin and Ethereum.
21 And as such, if you look at the -- you know, if
22 you start looking at Sai's metrics, I'm -- I'm
23 pretty sure it would not turn out well, in
24 comparison.

25 But what I'm implicitly doing here is

1 [REDACTED] - Highly Confidential

2 I'm -- I'm adopting the viewpoint that there is
3 decentralization at the network layer in all
4 cases; hence, let's look at the layers where
5 there is not.

6 This is -- this is the line of
7 thinking behind it.

8 Q. So just for completeness, which
9 blockchain layers did you leave out, or not
10 focus on, as part of the core focus of your
11 report?

12 MR. SYLVESTER: Objection.

13 A. So, I considered all the blockchain
14 layers and all the aspects. It is just that I
15 said, we opt to focus on decentralization
16 aspects of the system proper, and that says -- I
17 can read this out. To maintain emphasis on the
18 core distributed systems aspects.

19 In this report, we acknowledge these
20 decentralization aspects that go beyond the core
21 of a system, namely, network and application
22 layer decentralization. Yet we opt to focus on
23 decentralization aspects of systems proper.

24 Q. So, what are the core layers of a
25 system?

1 [REDACTED] - Highly Confidential

2 A. So the core layer is the -- what Sai
3 calls consensus layer, what I call resilience
4 layer. So this is the distributed systems
5 layer.

6 And then, I'm also focusing on
7 governance. Operational layer in Sai's case is
8 the part -- is part of my inclusiveness layer.

9 Maybe I should get -- taking it out,
10 but it's included.

11 So if you look at operational
12 decentralization, it's actually -- actually part
13 of -- it's part of inclusiveness. And openness.
14 In that context, I am discussing it.

15 So all the others are included,
16 incentive layer as part of in-protocol
17 incentives, governance layer.

18 Q. Okay.

19 I'm sorry, were you finished with your
20 answer?

21 A. Yes.

22 Q. Okay. Did you -- did you consider
23 every centralization factor for each layer,
24 putting aside network and application layer,
25 that Sai considered?

1 [REDACTED] - Highly Confidential

2 A. That Sai considered. Let's see, I --
3 storage constraint, specials equipment
4 concentration.

5 I discuss special equipment. I am
6 putting out as operational decentralization
7 storage constraints, as an example.

8 Wealth concentration of the incentive
9 layer I discussed in my report.

10 Consensus power distribution, so we
11 are discussing -- so for me, this is captured by
12 the resilience aspect. And there is owner
13 control and improvement control -- improvement
14 protocol, so these centralization factors that
15 he has, I'm considering in my report, I believe
16 all of them.

17 Q. Okay.

18 Would you agree that a reliable
19 measurement methodology is necessary before you
20 can compare different blockchain systems?

21 MR. SYLVESTER: Objection.

22 A. What does it mean "reliable" in this
23 case?

24 Q. Well, earlier, you spoke about
25 reliable as being replicatable results,

1 [REDACTED] - Highly Confidential

2 testable.

3 A. Yes. So, I -- in that sense, I -- I
4 believe it does, yes.

5 Q. Okay.

6 Are there any challenges in comparing
7 decentralization across different types of
8 blockchain systems?

9 A. If you take the Troncoso definition as
10 the basic point, so now again I need to read
11 through this, but if -- Troncoso definition is
12 very clear one. It sets the bar really low.

13 And for that, for me -- like the goal
14 of the -- of what one needs to show or not is
15 clear. Sometimes it is challenging to evaluate
16 what's really going on in the network.

17 One example is, you know, does one
18 authority control the interval mining pool, the
19 entire mining pool or not, and in that case, we
20 would make -- what I did in my report, I -- I
21 was trying to -- yeah, sorry, I lost it.

22 Q. Why don't -- that's fine. Why don't I
23 put a different question.

24 A. Yes.

25 Q. Your report offers an opinion that

1 [REDACTED] - Highly Confidential

2 bitcoin is a decentralized blockchain system.

3 Correct?

4 A. It does, yes.

5 Q. Does your opinion -- have you offered
6 an opinion in this case as to whether Ethereum
7 is decentralized?

8 A. I mentioned, in the report, that
9 Ethereum passes the Troncoso definition because
10 it doesn't have -- especially on the consensus
11 resilience layer, it doesn't have the trust in a
12 single authority.

13 So --

14 Q. Do you know where in your report you
15 say -- you say that Ethereum is a decentralized
16 blockchain system?

17 (Witness reviewing document.)

18 Q. I'll represent that I haven't seen it
19 written anywhere, so --

20 A. Probably -- it's probably
21 specifically, you're right. I don't think I
22 wrote it either.

23 Q. Was that in -- did you -- not -- was
24 that a purposeful or unintentional omission?

25 MR. SYLVESTER: Objection.

1 [REDACTED] - Highly Confidential

2 A. I was -- I think the question said to
3 what extent -- so I'm reading question for
4 expert opinion E1. To what extent is the
5 XRP Ledger centralized or decentralized when
6 compared to generally recognized blockchain
7 protocols such as those used by bitcoin and
8 Ethereum.

9 So I was not really asked to say
10 whether Ethereum is decentralized or not.

11 Q. So -- all right. Sitting here
12 today --

13 MR. SYLVESTER: Lisa, sorry to cut you
14 off. We've been going for about an hour
15 and a half. Is there a good time to take a
16 break?

17 MS. ZORNBERG: Yeah, let's break at
18 one o'clock.

19 MR. SYLVESTER: Does that work for
20 you, or are you hungry?

21 THE WITNESS: How much time there is
22 until 1?

23 MR. SYLVESTER: 20 minutes.

24 THE WITNESS: 20 minutes.

25 MR. SYLVESTER: He's on a different

1 [REDACTED] - Highly Confidential

2 time zone too. He's on Switzerland time
3 so --

4 MS. ZORNBERG: Can we continue till 1?

5 MR. SYLVESTER: If you need a break
6 right now, we can take a break right now.

7 THE WITNESS: Let's finish the
8 question and then break without going to --
9 to one o'clock. So just --

10 Q. Okay. So I'll finish this line of
11 questions.

12 A. Yes.

13 Q. Are you offering any opinion in this
14 case as to whether Ethereum is the decentralized
15 system?

16 A. I'm not.

17 Q. Do you have a view as to whether
18 Ethereum is decentralized?

19 A. I have a view. I have certain
20 opinions. And -- yeah. But I'm not offering
21 the opinion.

22 Q. In the past, have you cited to
23 Ethereum as an example of a -- of a blockchain
24 system that is totally decentralized?

25 MR. SYLVESTER: Objection.

1 [REDACTED] - Highly Confidential

2 A. To my recollection, I would never use
3 those words. No.

4 Q. Okay. I'm going to show one exhibit,
5 and we'll end on this -- on this point.

6 MS. ZORNBERG: Can we show Exhibit 8.

7 (Article titled [REDACTED]
[REDACTED]
[REDACTED] was

10 marked [REDACTED] Exhibit 8 for identification, as
11 of this date.)

12 Q. Do you recognize Exhibit 8?

13 A. I recognize it.

14 Q. This is a -- an article that -- that
15 you and your co-authors published in [REDACTED]
16 entitled, quote, [REDACTED]
[REDACTED]
[REDACTED]

19 A. Yes.

20 Q. Let me direct your attention to the
21 only part I'm going to ask you about. It's on
22 page 2 of the article, the first paragraph.

23 Can you read the first two sentences,
24 starting with, The blockchain may?

25 A. Second page? Where should I look? I

1 [REDACTED] - Highly Confidential

2 apologize.

3 Q. I'm holding it up. Just in case that
4 helps.

5 A. Okay. The blockchain may abide.
6 Right?

7 Q. Yes.

8 A. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

13 Q. Okay.

14 And you cite -- for the sentence that,

15 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

19 Can you tell me what -- what those
20 citations were?

21 A. This is Satoshi Nakamoto bitcoin paper
22 and Ethereum position white paper or yellow
23 paper by Gavin Wood. This is cited.

24 Q. Okay. So were you citing here to
25 Ethereum and bitcoin both as, Examples of

1 [REDACTED] - Highly Confidential

2 permissionless ledgers that are maintained
3 across peer-to-peer networks in a totally
4 decentralized and anonymous manner?

5 MR. SYLVESTER: Objection.

6 A. [REDACTED]

7 Q. Okay.

8 A. I'm a bit taken off guard here, so
9 this is not -- as you're writing the paper, it's
10 not a justification, but it's not something that
11 I would write. So maybe my co-authors write it
12 and it slipped through my cracks.

13 But this is definitely, you know,
14 totally decentralized for the purpose of this
15 paper, it's not even defined. So to understand
16 if something is totally decentralized and for
17 this paper to be clear on what's written here,
18 we would need to define what totally
19 decentralized means.

20 Q. Which you did not do in [REDACTED]

21 A. Which we didn't do for this --
22 practice of this paper, yes.

23 Q. Okay. But -- but do you agree that at
24 least as written in [REDACTED] you cited both to
25 bitcoin and to Ethereum as totally

1 [REDACTED] - Highly Confidential

2 decentralized?

3 MR. SYLVESTER: Objection.

4 A. Well, we cited, in this sentence, that

5 [REDACTED]

[REDACTED]

[REDACTED] we cite both

8 bitcoin and Ethereum, yes.

9 MS. ZORNBERG: Okay. We can take a

10 break.

11 THE WITNESS: Thank you.

12 THE VIDEOGRAPHER: It is 12:46 p.m.

13 We're going off the record.

14 (Luncheon recess at 12:46)

15

16

17

18

19

20

21

22

23

24

25

1 [REDACTED] - Highly Confidential

2 A F T E R N O O N S E S S I O N

3 (1:38)

4 [REDACTED] Ph.D.

5 resumed, having been previously duly
6 sworn by a Notary Public, was
7 examined and testified further
8 as follows:

9 THE VIDEOGRAPHER: It is 1:38 p.m. We
10 are back on the record.

11 CONTINUED EXAMINATION BY MS. ZORNBERG:

12 Q. Dr. [REDACTED] you testified earlier
13 that you view Troncoso's definition of
14 decentralization as setting a minimum floor for
15 a system to be decentralized.

16 Do you recall that?

17 A. Minimum -- low bar, minimum bar, let's
18 say.

19 Q. Minimum bar?

20 A. Yes, we can agree.

21 Q. Are you aware of any academic
22 literature that supports your view that Troncoso
23 sets a minimum bar for a system to be
24 decentralized?

25 A. I'm not aware -- I think I repeated

1 [REDACTED] - Highly Confidential

2 this at least two times. But I'm not aware of
3 any definition that would admit a decentralized
4 system if it doesn't satisfy Troncoso's
5 definition. So people, while they're proposing
6 definition of decentralized systems, they might
7 not cite Troncoso, you know. Just cite that
8 paper.

9 But they might come to the similar,
10 stronger test that would admit a system is
11 decentralized. So this is what I'm saying.

12 Q. Do you have -- I understand.

13 Do you have in mind, though, any
14 literature -- scientific literature, that does
15 cite the Troncoso definition or standard and
16 agrees or acknowledges that that sets a minimum
17 bar for decentralization?

18 A. Well, there is at least my paper that
19 does it.

20 Now, whether explicitly, no -- well,
21 one way to find it out would be to go to
22 Google Scholar to look at the citations of the
23 Troncoso and to basically make sure if somebody
24 actually declares this as the -- as the thing.

25 Q. Did you do that work in preparing your

1 [REDACTED] - Highly Confidential

2 report?

3 A. I didn't go through 50-something
4 citations of Troncoso in order to do that.

5 Q. Okay. All right. Moving to another
6 subject.

7 Are you offering any opinion in this
8 case regarding how the term "decentralized" has
9 been used by the SEC as relates to blockchain
10 systems?

11 A. I do not.

12 Q. Okay.

13 A. That wouldn't be fair, no.

14 Q. I take it, then, you're also not
15 offering an opinion regarding what any SEC
16 employee may have meant or not in using the term
17 "decentralized"?

18 A. That is correct.

19 Q. Okay. More broadly, are you offering
20 an opinion about how any United States
21 regulators have used the term "decentralized"?

22 A. I'm definitely not an expert on U.S.
23 regulations. And, no, I'm not doing that.

24 Q. Do you know if the SEC has ever cited
25 to the Troncoso paper prior to bringing its

1 [REDACTED] - Highly Confidential

2 lawsuit against Ripple?

3 A. No. So -- if I rephrase the question,
4 did SEC in any public or speech known to me --
5 maybe it's not public -- refer to the Troncoso
6 paper before, let's say, me introducing it? The
7 answer would be no.

8 DIR Q. As far as you know, did you introduce
9 that paper and its definition of decentralization
10 to the SEC through your work on this case?

11 MR. SYLVESTER: Objection.

12 That might be getting into privileged
13 communications.

14 And I -- I'm going to ask you not to
15 answer that one.

16 Q. Sitting here today, as far as you
17 know, Dr. [REDACTED] did anyone at the SEC know of
18 the Troncoso definition before you yourself
19 found it while digging into this case in the
20 summer of 2021?

21 MR. SYLVESTER: If you know.

22 A. That I couldn't know. So --

23 Q. Okay.

24 A. -- yeah.

25 Q. Do you know if the SEC has ever

1 [REDACTED] - Highly Confidential

2 defined the term "decentralization" for purposes
3 of securities regulation?

4 A. I don't know if they did, which means
5 they could or not, but not that I know.

6 Q. Okay. And you don't know if the word
7 "decentralized" appears in United States
8 securities laws or regulations?

9 A. I really don't know that, no.

10 Q. Are you offering any opinion in this
11 case as to whether decentralization is relevant
12 to the legal definition of an investment
13 contract, under securities law?

14 A. I'm not offering that opinion.

15 Q. Okay. Are you aware that the SEC
16 produced documents in this case, reflecting its
17 communications about decentralization with
18 blockchain market participants?

19 MR. SYLVESTER: Objection.

20 A. I'm not sure I understand the
21 question. If you rephrase, maybe I can relate.

22 Q. Yeah, yeah, sure.

23 Do you know whether the SEC, in this
24 lawsuit, has turned over documents from its own
25 files, reflecting its discussions with people in

1 [REDACTED] - Highly Confidential

2 the -- in the blockchain industry, about
3 decentralization?

4 MR. SYLVESTER: Objection.

5 A. Yeah. The -- to my understanding of
6 the question, that would be no. So I'm not --
7 I'm not aware of that. No.

8 Q. Okay.

9 Let me show you [REDACTED] -- Exhibit [REDACTED] 9.

10 (Tweet from Neha Narula was marked [REDACTED]
11 Exhibit 9 for identification, as of this
12 date.)

13 Q. I think we discussed earlier this
14 morning, that you -- you recognize the name,
15 Neha Narula from conferences in the blockchain
16 industry, right?

17 A. I recognize the name, yes.

18 Q. Okay. Do you know that she's the head
19 of MIT's digital currency lab?

20 A. I know she's affiliated with MIT. I
21 didn't know the -- what's the word? So I didn't
22 know the -- which role she has at MIT, which
23 position she has.

24 Q. Is the MIT digital currency lab part
25 of the scientific community studying blockchain?

1 [REDACTED] - Highly Confidential

2 A. That's a good question. So I -- so
3 MIT certainly is. Let's not go there. Right?

4 Was the status of the MIT this and
5 that, what is their status in the community?
6 In -- at MIT, that I don't know in details.

7 Q. Okay.

8 A. Know that Neha Narula writes
9 scientific papers. They're not on my immediate
10 radar. So I'm not, you know, often seeing her
11 papers.

12 Q. Okay.

13 A. Does that make sense?

14 Q. Sure.

15 So I'm -- Exhibit [REDACTED] 9, is a tweet by
16 Neha Narula, from June 15, 2018. I'll just read
17 it for the record.

18 It says, quote, I'm a little worried
19 people from government agencies are throwing
20 around the word "decentralization" like we know
21 what it means or how to evaluate it.

22 Closed quote.

23 Have you previously seen this tweet?

24 A. I might have.

25 Q. Do you follow Ms. Narula on Twitter?

1 [REDACTED] - Highly Confidential

2 A. No.

3 Q. Okay.

4 Do you know what Ms. Narula was
5 referring to here when she stated that
6 government agencies are throwing around the word
7 "decentralization"?

8 A. I really do not know what she referred
9 to. I don't know that. I don't know what's
10 "we" referring to.

11 Q. Okay.

12 A. Who is "we" referring to?

13 Q. Have you personally read any speeches,
14 or publications, by SEC officials, relating to
15 the issue of cryptocurrency?

16 A. Speeches? How do you define speeches,
17 or -- have I read speeches?

18 Q. Let's start with speeches. Have you
19 read any speeches by the SEC relating to the
20 issue of decentralization?

21 MR. SYLVESTER: Objection.

22 THE WITNESS: Yes.

23 A. So to my understanding, I did not, so
24 no.

25 Q. No. Okay. I'll represent to you that

1 [REDACTED] - Highly Confidential

2 Ms. Narula tweeted out this tweet in Exhibit 9
3 one day after an SEC official gave a speech
4 discussing decentralization of blockchain
5 systems.

6 Do you -- do you agree with the
7 concern Ms. Narula's tweet expresses that
8 members of -- that -- that people from
9 government agencies are throwing around the word
10 "decentralization"?

11 MR. SYLVESTER: Objection.

12 A. I don't know in which sense throwing
13 around, so I would not agree with "throwing
14 around," the word.

15 Does that help?

16 Q. Okay. Are you involved in any of your
17 work in advising -- putting aside your work as
18 an expert in this case, have you ever advised
19 United States regulators on the meaning of
20 decentralization?

21 A. No, I have not.

22 Q. Okay. You can set that aside.

23 Is the -- is the term "sufficiently
24 decentralized" a term that has any meaning to
25 you?

1 [REDACTED] - Highly Confidential

2 MR. SYLVESTER: Objection.

3 A. It has certain meaning.

4 It has certain meaning. Yes.

5 Q. What does sufficiently decentralized
6 mean?

7 A. I'm not sure. So I -- the term might
8 mean something. I'm not sure.

9 Q. You're not sure?

10 A. Yes. So -- yeah. Sufficiently could
11 be -- I can speculate.

12 Q. I'm not asking you to speculate.

13 A. Very good.

14 Q. Okay. But I guess my question is, in
15 your experience, is there -- is there any
16 scientific standard that you've seen, for
17 determining when a blockchain system is,
18 quote/unquote, sufficiently decentralized?

19 MR. SYLVESTER: Objection.

20 A. We spent a lot of time today
21 discussing the minimum and basic condition which
22 would go out for necessary decentralization.

23 Sufficient decentralization would
24 probably be a spectrum of things that would mean
25 different things to different people. I think

1 [REDACTED] - Highly Confidential

2 this is the only fair thing to say.

3 Q. Okay.

4 A. So I admit -- I admitted permission
5 blockchains decentralized according to the
6 Troncoso definition and methodology that I'm
7 following. I'm pretty sure there are people
8 around who would say that no permission
9 blockchain is decentralized.

10 Q. Are you offering any opinion in this
11 case on the -- what "sufficiently decentralized"
12 means?

13 Sounds like you're not.

14 A. I'm not. I have my opinion, but I'm
15 not offering it. Does that make sense?

16 Q. Okay.

17 Are you offering any opinion in this
18 case on how the SEC or any employee of the SEC,
19 has used the term "sufficiently decentralized"?

20 A. I do not.

21 Q. Okay. When does a blockchain system
22 become operational, in your view?

23 MR. SYLVESTER: Objection.

24 A. That's -- you need to define
25 "operational," to start with.

1 [REDACTED] - Highly Confidential

2 Q. So does -- does the term "operational"
3 have one set meaning to you?

4 A. Operational, no, it does not. So
5 operational could be something that works. Does
6 it work as intended? That's one question.

7 Do I call that operational? Or you
8 just -- it works and not necessarily is it
9 intended, is it that operational? So that's
10 basically what I'm struggling immediately.
11 There might be other things which I'll be
12 struggling with.

13 Q. Okay. If a -- if a blockchain system
14 works as intended, would you agree that it's
15 operational?

16 A. That could be one -- if operational
17 is -- if the word "operational" means that, then
18 I guess answer could be yes.

19 Yeah.

20 Maybe.

21 Q. Okay.

22 A. Maybe. It depends on the definition
23 of the word "operational." So operational, work
24 as intended, so what does it mean "intended"?
25 So I guess there is specification, and the

1 [REDACTED] - Highly Confidential

2 system is proven to do that thing.

3 Q. So let me -- let's take an example.

4 Let's take an example.

5 How soon after the bitcoin network
6 launched did it become operational, in your
7 view?

8 MR. SYLVESTER: Objection.

9 A. We would need to define what operation
10 of a bitcoin means. Shall we try to do it? Or
11 no?

12 Q. What do you think operational for a
13 bitcoin means?

14 A. I don't know. You came up with the
15 word. I really don't -- I'm not using the word.
16 Yeah.

17 Q. Well, actually -- I'm not meaning --
18 this is -- I'm trying to get your understanding,
19 of whether -- whether it has a scientific
20 meaning. I -- whether the term "operational" --
21 how is it applied to discussions of blockchain
22 systems, if at all?

23 I don't want you to assume any
24 definition I'm giving it. I'm asking you if it
25 has meaning to you to discuss when a blockchain

1 [REDACTED] - Highly Confidential

2 system becomes operational.

3 MR. SYLVESTER: Objection.

4 Go ahead.

5 A. Yes. I believe that it doesn't

6 have -- determined meaning to me. So --

7 Q. Okay.

8 A. -- I would really then go -- if

9 somebody -- if you were not you but just my

10 colleague comes to me and comes with the same

11 question, I would say, What do you mean by

12 "operational"?

13 And then we would probably engage in a

14 discussion of what "operational" means.

15 Q. Okay. Understood. So there's no --

16 okay.

17 Does the -- is the term "fully

18 functional" a term that has any meaning to you

19 in describing blockchain systems?

20 MR. SYLVESTER: Objection.

21 Go ahead.

22 A. Yeah. In some sense it is similar to

23 operational. Again, we need to define "fully

24 functional," so I guess there is a function of

25 the blockchain, again, which relates to the

1 [REDACTED] - Highly Confidential

2 specification.

3 And then "fully" would be -- yeah,
4 there are no missing features. It is really
5 like what it's doing? What specification is
6 supposed to tell the people that they're doing?
7 And there are no bugs whatsoever.

8 This is how I would reason. But I'm
9 online reasoning. You asked me the question. I
10 just gave you online opinion about it.

11 Q. I see. Before sitting here today in
12 this deposition, have you given thought to
13 whether the term "fully functional" has a
14 definition to the scientific community?

15 A. In this wording, "fully functional,"
16 no, I am not.

17 Q. Are you offering any opinion in this
18 case on the definition of fully functional as
19 relates to blockchain systems?

20 A. I do not.

21 Q. I think we -- we discussed this
22 morning that the development of distributed
23 networks can involve iterative processes with
24 changes over time. Right?

25 A. Yes.

1 [REDACTED] - Highly Confidential

2 Q. Can a blockchain system be operational
3 even if additional development happens --

4 MR. SYLVESTER: Objection.

5 Q. -- over time on that system?

6 MR. SYLVESTER: Objection.

7 A. It, again, goes back to the definition
8 of operational. Since we didn't agree on the
9 definition of the word, I presume there is a
10 world in which there is a definition of
11 operational that would permit your example.

12 Q. Well, let's use -- let's talk -- let's
13 use for a minute the concept of operational that
14 it works as intended.

15 A. Okay.

16 Q. Okay. Do you have a view on when --
17 when the bitcoin network became operational?

18 A. I'm not aware of the full
19 specification of bitcoin as operating as
20 intended.

21 You could say -- so depending on the
22 standpoint you take, if the specification is the
23 code, then it's always operating as intended.
24 If there is a separate specification from the
25 code, you would need to establish -- and I'm not

1 [REDACTED] - Highly Confidential

2 aware that there is a, for example, separate
3 specification of bitcoin code apart from the
4 code itself.

5 Q. Okay.

6 A. So if you take a standpoint -- now I'm
7 really coming with this online. If you come
8 with the standpoint that the code itself is the
9 specification, then it's fully operational,
10 yeah. It's just doing what the code tells it to
11 do.

12 Q. I see.

13 A. Yeah, so --

14 Q. So if the -- if bitcoin was launched,
15 and it operated as imagined and intended based
16 on its code, one could say it was operational
17 immediately when the code launched.

18 MR. SYLVESTER: Objection.

19 A. If this is the definition. If what
20 the code does is -- is the specification, what
21 the code should be doing and you would call this
22 operational, then the answer is yes.

23 Q. Okay.

24 A. There would be other definitions of
25 operational for which the answer would be no.

1 [REDACTED] - Highly Confidential

2 Notably when the -- as intended is separate from
3 the code.

4 Q. Are you expressing any view in this
5 case as to when the XRP Ledger became
6 operational?

7 MR. SYLVESTER: Objection.

8 A. I'm coming back to the ambiguity of
9 the word "operational," so I guess my answer
10 would be no.

11 Q. And are you also not expressing any
12 opinion in this case on when the XRP Ledger
13 became fully functional, a term which you've
14 also said is -- is vague?

15 MR. SYLVESTER: Objection.

16 A. I -- again, so I'm relating to the
17 fact that we would need to define this notions
18 fully. And, I'm not offering any opinion on
19 that. So I'm not -- I think we're going -- so
20 correct me, but I think we're going a bit in a
21 circle, but I'm just repeating what I did. So
22 yes.

23 Q. Okay.

24 A. I'm not offering any.

25 Q. Let's move on. I want to just -- here

1 [REDACTED] - Highly Confidential

2 is what I would like you to explain, though.

3 When a blockchain system is launched
4 and it's being used and it's being used in the
5 way that it was intended to be used, can
6 additional functions still be added to that
7 blockchain later?

8 MR. SYLVESTER: Objection. Objection.

9 A. So it is working and it's working as
10 it's supposed to be working. And you're adding
11 other things, which means that you're adding
12 things that it was not how it was supposed to be
13 working.

14 Right?

15 Q. I'm just asking how -- maybe I'm --
16 let me simplify. Isn't it very common for
17 operating blockchain systems, for developers to
18 continue adding added functions and features to
19 those already operating blockchain systems?

20 MR. SYLVESTER: Objection.

21 A. Again, so the operating -- operating
22 as running, so there is a code that's running on
23 the nodes. And blockchain developers add the
24 codes to the software. And it's updated
25 regularly. Yes, this is a commonplace, of

1 [REDACTED] - Highly Confidential

2 course, yes.

3 Q. Okay. I would like to turn back now
4 to talking about UNLs an the XRP Ledger.

5 Are participants in the XRP Ledger
6 ecosystem required to use the UNL published by
7 Ripple?

8 MR. SYLVESTER: Objection.

9 A. They are not required. To use the UNL
10 published by Ripple.

11 Q. Can a participant modify their
12 instance of rippled to use a UNL other than the
13 default UNL?

14 A. They can do that, yes.

15 Q. Okay. So, for example, can an
16 XRP Ledger participant modify their instance of
17 rippled to exclude all Ripple-operated
18 validators from their UNL?

19 A. The -- a validator could do that, yes.

20 Q. How would they accomplish that
21 modification?

22 A. They would -- you -- it can be done in
23 different ways. You could download the UNL from
24 the Ripple site, basically just go and exclude
25 those validators. That's one way to do it.

1 [REDACTED] - Highly Confidential

2 Q. Okay. And would a validator be
3 required to obtain permission from Ripple before
4 making that modification?

5 A. No. It wouldn't.

6 Q. Would they be required to obtain
7 permission from any third party before making
8 that modification?

9 MR. SYLVESTER: Objection.

10 Q. You can answer.

11 THE WITNESS: Yes.

12 A. So to my understanding, no.

13 Q. Could a participant write their own
14 code to perform all XRP Ledger functions?

15 A. There is nothing preventing the -- the
16 client to write a compatible code, not in C, but
17 in some other language, for example. Why not?
18 Yes.

19 Q. Okay. And if -- if other -- if others
20 on the XRP Ledger decided to trust someone or
21 persons other than Ripple, could Ripple do
22 anything to stop that --

23 MR. SYLVESTER: Objection.

24 Q. -- to your knowledge?

25 MR. SYLVESTER: Objection.

1 [REDACTED] - Highly Confidential

2 A. To my understanding, no. Now, we are
3 entering the field in which we need to
4 understand. So, you know, we said we can -- can
5 you change the software? Can you do this? Can
6 you do that?

7 The question is what guarantees you
8 have once you do that. So we should probably at
9 some point discuss that.

10 But to come back to your question, the
11 answer is, normally, there is no permission or
12 third party for me, as a validator in the Ripple
13 network, to modify my software. I can do that
14 as I please.

15 Q. By "guarantees," are you referring to
16 guarantees of liveness and safety?

17 A. That's it.

18 Q. Okay. Well, we're going to get to
19 that shortly.

20 As of the date of your report, how
21 many XRP Ledger participants used the UNL
22 published by Ripple, if you know?

23 A. That I don't. I don't know.

24 Q. Okay. Do you know how many XRP Ledger
25 participants used a UNL different than the one

1 [REDACTED] - Highly Confidential

2 published by Ripple as of the date of your
3 report?

4 A. That I don't know.

5 Q. I don't take it -- let me rephrase.

6 Are you asserting that every
7 XRP Ledger participant uses the UNL published by
8 Ripple?

9 A. I'm not asserting that.

10 Q. Did you speak to any XRP Ledger
11 validator in preparing your report?

12 A. Validator operator. Not -- yeah.

13 No. No, I did not. Validator would
14 be software, but, yeah. So --

15 Q. Okay.

16 A. I cannot speak to the software, but
17 operator --

18 Q. Okay. I understand. Okay. Thank you
19 for that correction.

20 So did you -- did you -- so let me --
21 did you speak to any XRP Ledger node operator in
22 preparing your report?

23 A. I did not.

24 Q. Do you have any basis to conclude that
25 every XRP Ledger participant uses the UNL

1 [REDACTED] - Highly Confidential

2 published by Ripple?

3 A. I did not offer that conclusion, as we
4 discussed.

5 Q. Okay. All right. So -- so let's turn
6 now to the subject of resilience, which is
7 the -- one of the four decentralization aspects
8 you discuss in your report. Right?

9 Let me direct you to page 9 of your
10 report, please.

11 So, first, in the context of your
12 report's methodology, what is resilience?

13 A. Resilience of the system refers to
14 ability to withstand Byzantine behavioral
15 components of the system.

16 Q. Okay. And what is that definition
17 based on?

18 A. That definition is based on the use of
19 the word "resilience" in almost all papers I
20 know about which deal with Byzantine
21 Fault-Tolerant protocols and blockchain
22 protocols. So all of them would be having an
23 assumption on the adverse side that the protocol
24 can tolerate and still provide its guarantees.

25 For different concerns with protocols,

1 [REDACTED] - Highly Confidential

2 this may come up in different flavors. You --
3 in proof-of-work protocols, it would be
4 expressed as a percentage of the mining power
5 that needs to be controlled in order for the
6 adversary to be stopped if it controls less than
7 that threshold or for adversary to succeed in
8 mounting an attack to the system as I'm
9 describing later.

10 In the group of Byzantine
11 Fault-Tolerant protocols or just the protocols
12 that vote by -- like one validator/one vote, or
13 weighted voting, such as in proof of state, you
14 weight -- you vote with your stakes or the more
15 stake you have, the higher the value of your
16 vote.

17 That would be a different -- this --
18 this also, the resilience threshold also
19 appears. And it denotes the number of
20 components or, like, number of validators, if
21 you want, in the system, that -- which you can
22 turn to the fraction, if you have a snapshot of
23 the behavior of the membership of the current
24 system. You can relate to the fraction as well.

25 So we discussed before in this

1 [REDACTED] - Highly Confidential

2 deposition for -- just to give an example, we
3 discussed about one-third, up to one-third of
4 nodes, up to one-half of nodes, et cetera.

5 These are all impacting the resilience of the
6 system. So that number, that critical number of
7 Byzantine needs, that would be the number of
8 tolerated.

9 Q. And when you refer -- when you refer
10 to that critical number --

11 A. Yes.

12 Q. -- are you referring to the Nakamoto
13 coefficient or something else?

14 A. So I'm referring to -- I point you to
15 page 9.

16 Q. Yes.

17 A. So this is the last paragraph in the
18 resilience section.

19 So I will read it out. So I say, In
20 this context, the scientific literature and
21 engineering practice is typically interested in
22 the minimum number of authorities that the
23 adversary needs to compromise to subvert the key
24 property of a system, such as safety and
25 liveness, full stop.

1 [REDACTED] - Highly Confidential

2 So I'm referring to minimum number of
3 authorities. And when I say "scientific
4 literature and engineering practice," I don't
5 give exact.

6 Q. Okay. In the next sentence, though,
7 you say that this number is sometimes referred
8 to as the Nakamoto coefficient.

9 A. Yes. As you see, this is a mouthful.
10 The first sentence is a mouthful. So since --
11 let's call it some way. And then I was
12 considering -- honestly, when I was writing
13 this, I was considering two things.

14 One, I call it coefficient of
15 Byzantine nodes. And then I saw that some
16 people who are in the space call that and also
17 define that notion, and then you use it in the
18 definition as Nakamoto coefficient.

19 I said, Okay. This is nice. This is
20 not mouthful. It's interesting and may grab
21 people's attention. Let's call it this way.

22 What it means is basically defined in
23 the previous sentence.

24 Q. Okay. So prior to your work on the
25 case, were you familiar with the term "Nakamoto

1 [REDACTED] - Highly Confidential

2 coefficient," or is that a term that you
3 encountered while doing work on this case?

4 A. So I -- I was aware that people use
5 it. I didn't use it in my work. I would
6 usually refer to this threshold as the number of
7 potentially Byzantine participants, which,
8 again, for the presentation, because one of
9 the -- when I was writing this report, one of
10 the guidelines, so -- so -- that came up is this
11 should be readable for nontechnical audience.

12 So I was trying to come up with a term
13 that would -- you know, that I would use to
14 refer to this notion without calling it
15 coefficient of, you know, the threshold on the
16 number of Byzantine nodes, which is again --

17 Q. Okay.

18 A. So I was aware of the -- of the term.
19 I didn't use it much. I thought it would be
20 nice for -- for a report that supposed to be
21 read by nonexpert to call it that way.

22 Q. Can a system be resilient but
23 centralized?

24 MR. SYLVESTER: Objection.

25 A. So resilient in the -- so resilient in

1 [REDACTED] - Highly Confidential

2 the context of my report, the way I'm defining
3 things here, it could -- so some components of
4 the system, at some layers, you could have a
5 ability to tolerate Byzantine faults; but at
6 some other layer, for example, you do not.

7 So you need to understand, if we
8 discuss the network layer versus distributed
9 systems layer, right? So we could have a
10 centralization on either of the two, and it's
11 really an end to call it decentralized.

12 Q. It's really a?

13 A. End function, end function.

14 Q. End, E-N-D?

15 A. Yes. So if it is decentralized at a
16 consensus and the distributed systems layer, it
17 would also need to be decentralized at the
18 network layer would probably be centralized.

19 Q. Okay. But coming back to question,
20 can a distributed blockchain system be resilient
21 but centralized?

22 MR. SYLVESTER: Objection.

23 A. So let's read this as -- as -- as I
24 specified here. So resilience, if this is the
25 ability to withstand behavior of certain

1 [REDACTED] - Highly Confidential

2 components of the system, you could have a
3 system that's -- is able to do so. But it's
4 still centralized because of the -- when we come
5 to the minimum number of authorities that the
6 adversary needs to compromise to subvert key
7 property in the system, this would still be one
8 because there is, for example, some specific
9 component of the system from which you can mount
10 an attack --

11 Q. So the answer is yes --

12 A. -- so probably yes. Probably could be
13 yes.

14 MR. SYLVESTER: Let me finish the
15 answer, please.

16 Q. Please.

17 A. I believe the way you pose the
18 question, the answer would probably be yes, yes.

19 Q. Okay. Can a system be decentralized,
20 but not resilient?

21 A. No. I would say the answer is no.

22 Q. No.

23 So a system must be resilient in order
24 to qualify as a decentralized system.

25 A. Yes.

1 [REDACTED] - Highly Confidential

2 Q. Okay. How do you measure resilience?

3 A. So we measure resilience, using this
4 minimum number of authorities that the adversary
5 needs to comprise to subvert the key property of
6 the system, such as safety and liveness. In the
7 context of blockchain, this number is sometimes,
8 sometimes referred to as Nakamoto coefficient.

9 So that -- and as the text says later,
10 the higher the Nakamoto coefficient, the higher
11 the level of decentralization.

12 As per the definition of a
13 decentralized system, we adopted, I'm citing
14 Troncoso, if this number is one, which means if
15 a single participating authority can compromise
16 a key property of the system, the system cannot
17 be decentralized.

18 MS. ZORNBERG: Okay. Let the record
19 reflect that Dr. [REDACTED] was reading almost
20 verbatim from a paragraph on the middle of
21 page 9 of his report.

22 Q. Right?

23 A. Yes, that is correct.

24 Q. Okay. Are you familiar with the
25 concept of partition tolerance in blockchain

1 [REDACTED] - Highly Confidential

2 systems?

3 A. I am.

4 Q. What is partition tolerance?

5 A. Partition tolerance, we mentioned it
6 briefly, at the second, I believe, hour of the
7 deposition. It's related to this
8 asynchronous --

9 Q. This what?

10 A. Asynchrony, asynchronous, I was
11 telling this --

12 Q. Oh.

13 A. Yes. So it's related to that.

14 So when the network exhibits
15 asynchrony, we also call it network partitions,
16 which means if my message is there, I'm trying
17 to send a message to you and it takes a long
18 time. And network partition is this temporary
19 inability for you and me to communicate.

20 So some -- in some communities, this
21 would be called asynchrony, asynchrony. And in
22 some others, it would be called network
23 partition. Usually refer to the same thing.

24 Q. Is partition tolerance an element of
25 the resilience of a system?

1 [REDACTED] - Highly Confidential

2 MR. SYLVESTER: Objection.

3 A. That depends on the stated goals of
4 the system, some -- some systems might opt -- so
5 any system, when you discuss the -- any systems
6 comes with a specification. So it should come
7 with a specification that it's doing something
8 assuming this, this, and that.

9 So if I can devise a system in which I
10 am not tolerating network partitions and that
11 would be fine so long, you know, I'm designing
12 such a system.

13 Q. Okay, so, you would agree that -- a
14 blockchain system can opt by design, to either
15 be partition tolerant or not partition tolerant.

16 A. It could. Yes.

17 Q. Okay. So would you agree that a
18 partition-tolerant blockchain is vulnerable to
19 an involuntary fork?

20 A. Partition-tolerant system is
21 vulnerable to involuntary fork -- can you repeat
22 your question.

23 Q. Yes. Is a partition-tolerant
24 blockchain vulnerable to an involuntary fork?

25 A. Not necessarily.

1 [REDACTED] - Highly Confidential

2 Q. Does that mean maybe?

3 A. Maybe.

4 Q. So a partition-tolerant blockchain
5 system can be vulnerable to an involuntary fork?

6 A. It can be -- well, so involuntary,
7 now, we need to dive into -- yes, it's
8 definitely -- I -- it goes both ways. Both --
9 both worlds are possible.

10 Q. Okay. Why didn't you mention
11 partition tolerance anywhere in your report?

12 A. Oh, I did.

13 Q. Oh, where?

14 A. I'm, like, whole my Appendix B. Whole
15 my Appendix B is dealing with partitions. So,
16 basically, I'm describing an attack to the -- to
17 the -- XRP Ledger. This is assuming -- so this
18 is apart from a dUNL. DUNL works correctly.
19 The validator list site publishes consistently
20 the same, UNL stored nodes. And now you can
21 mount an attack in which you also introduce
22 partitions to the network.

23 Q. Okay.

24 A. So that part is actually relying on
25 that, and I call that unreliable network.

1 [REDACTED] - Highly Confidential

2 So now we talked about the asynchrony.
3 We talked about partition network. And another
4 way to say unreliable network. So you see,
5 page 33, Appendix B, the third bullet, The
6 network is called unreliable if it can drop and
7 delay messages exchanged among correct
8 validators. This is what I was trying to --

9 Q. I see that.

10 Now, Appendix B that you're pointing
11 out here relates solely to scenarios for the
12 XRP Ledger.

13 Correct?

14 A. Correct.

15 Q. Did your report talk about partition
16 tolerance in relation to the bitcoin network?

17 A. My report did not talk about partition
18 tolerance for the bitcoin network.

19 Q. Why not?

20 A. It's designed to -- one way to think
21 about it is that, bitcoin network is meant
22 for -- so the way it was built is that nodes can
23 proceed independently from each other, if
24 they're on the network partition. And that's by
25 the feature of -- by the virtue of the -- that's

1 [REDACTED] - Highly Confidential

2 a feature -- that's actually -- you know, if we
3 talk about operating as intended, this is
4 operating as intended.

5 Q. So are you familiar with the CAP
6 theorem?

7 A. I am.

8 Q. Okay. What's the CAP theorem?

9 A. CAP theorem is the basic distributed
10 computing theorem that says that consistent --
11 CAP stands for consistency, availability, and
12 partition tolerance. It's one way of stating --
13 restating the official Lynch-Patterson
14 consultancy possibility result.

15 MS. ZORNBERG: Hold on.

16 Did you get that?

17 THE COURT REPORTER: I flagged it for
18 a spelling. I will get the spelling later.

19 THE WITNESS: Thank you.

20 MS. ZORNBERG: Okay.

21 A. So it's another way to say that
22 systems essentially if they're subject --
23 especially consensus systems, if they're subject
24 to network partitions, they need to opt by
25 design what property they will favor, when this

1 [REDACTED] - Highly Confidential

2 partition network happens.

3 By the way, again, as we discussed,
4 you can design a system in which you opt not to
5 tolerate partitions. This is usually
6 ill-advised because partitions happen or not
7 without your control. So they could happen
8 just -- so now if you accept that partitions can
9 happen, what the CAP theorem says is that the
10 designer can pick, like on a high level, one --
11 two out of three properties.

12 Q. Two out of three. So the CAP theorem
13 basically posits that there are trade-offs in
14 designing --

15 A. Yes.

16 Q. -- distributed systems?

17 A. Yes.

18 Q. What does it mean -- let me rephrase.

19 Focusing on bitcoin for a moment, does
20 bitcoin have partition tolerance?

21 A. It does.

22 Q. Are operational bitcoin nodes aware of
23 whether they can reach all other operational
24 bitcoin nodes?

25 A. I don't know. Normally they don't

1 [REDACTED] - Highly Confidential

2 know all matters. They don't even attempt.

3 They usually sample the population of the whole

4 network. So you're not -- in such a network,

5 you're not even aware of how many nodes there

6 are. So as such, you're not able to tell, can

7 you reach all of the other nodes or not, because

8 you're not even attempting.

9 Q. Okay. So -- so let me give you an
10 example.

11 A. And you couldn't -- and you couldn't.

12 Q. Let me give you an example. If there
13 were a eruption to the Internet connection
14 between two countries, Country A and Country B,
15 would bitcoin nodes operating in Country A know
16 they could no longer reach nodes operating in
17 Country B?

18 A. If they tried to reach them, they
19 would know that they cannot.

20 Q. Through human contact?

21 A. No, not necessarily. If I'm
22 connected, you know, if I know I'm connected to
23 this and this IP address, then I can figure out
24 that I am talking -- that this site here is --
25 is belongs to that country. I could basically

1 [REDACTED] - Highly Confidential

2 understand that my connection doesn't work. You
3 can detect that in software.

4 Q. Okay. So sticking with the same
5 example, if Alice submitted her transaction in
6 Country A during a time when Country B was
7 experiencing an Internet disruption, would her
8 transaction be excluded from the bitcoin
9 blockchain in Country B?

10 A. That really depends. So if network --
11 if Country A doesn't -- is unable to talk
12 directly to Country B, because bitcoin operates
13 on a gossip network, it might happen that there
14 is a connection from A to B which goes via C,
15 Country C. So A and C can -- A and C can talk.
16 B and C can talk. And hence, you know, if
17 subnetwork of -- that belongs to Country A of
18 the miners that are located in Country A, they
19 mine a bitcoin, they mine a block, they could be
20 able to reach Country B, by the --

21 Q. Country --

22 A. Not necessarily. In a -- let's assume
23 that the network splits in two, and then we can
24 discuss that if you want to.

25 Q. Okay. Is it -- is it possible -- to

1 [REDACTED] - Highly Confidential

2 that example, is it also possible, that in the
3 example I gave where there's an Internet
4 disruption and Alice puts in her transaction in
5 Country A, is it possible that bitcoin nodes in
6 Country A, and Country B, would continue
7 operating and adding new blocks independently?

8 A. There is a possibility. If the
9 network is split into distinct parts that are
10 completely unable to talk to each other, it is
11 possible that the blockchain advances
12 independently. Yes.

13 Q. That would be a fork?

14 A. That would be -- so at the -- at that
15 moment, if you have a God's view on the system,
16 you would call it a fork. At that moment, these
17 nodes are not aware. They would be aware of --
18 so there are a lot -- lots of meanings of forks
19 in this world, right? So this would be a fork
20 on the blockchain as a data structure. Right?

21 Only when it comes together. So, once
22 the network partition heals, these nodes start
23 talking to each other. And how the bitcoin
24 system is designed is it was actually
25 designed -- the desired operation in that case

1 [REDACTED] - Highly Confidential

2 is that, when the network partition heals and
3 nodes start talking to each other, bitcoin
4 network just falls to this -- which longer fork.
5 Basically, there is a history, this is
6 Network A's blocks. This is Network B's blocks.
7 You will take the longer one and default to that
8 one -- not default, but actually the network
9 reaches consensus on one of the two histories.

10 Q. Is any human intervention required to
11 prevent a fork in the situation that we've been
12 discussing?

13 A. We didn't discuss preventing the fork.
14 But all what I described -- to maybe answer
15 question, in all what I described no human
16 intervention is needed.

17 Q. Okay. All right. On page 9 of your
18 report, you talk about safety. And it looks
19 like you basically explain that safety
20 stipulates that bad things do not happen.

21 A. Yes.

22 Q. What is that based on, that definition
23 based on?

24 A. My first -- the first time I
25 encountered these two notions when Rachid

1 [REDACTED] - Highly Confidential

2 Guerraoui was teaching these notions --

3 Professor Rachid Guerraoui at EPFL was teaching
4 these notions back in 2003. He used this
5 wording. And this is common wording across
6 scientific papers and across, you know, in
7 different course, et cetera.

8 This is the way to explain on
9 extremely high level. To give an intuition
10 again, the wording here was adopted for the
11 audience. And this is -- the one that even was
12 used in introductory courses to us, as
13 distributed systems designers. So, you know,
14 this is a common thing to do. I didn't use it
15 for the first time myself.

16 Q. Okay. Would you agree it's a good
17 thing for a decentralized system to be safe?

18 MR. SYLVESTER: Objection.

19 A. We need to define "good," actually.
20 So honestly, diving into that, it's a
21 philosophical thing in the design of the system.
22 For example, I was a lot -- spending a lot of my
23 time working on systems that favor in the CAP
24 theorem. So partition hits you and now you're a
25 system designer picking one of the two.

1 [REDACTED] - Highly Confidential

2 So, we -- it turns out, to certain
3 extent, this was the intention. The way I
4 understand the XRP Ledger concerning this
5 protocol, this was the intention of XRP Ledger
6 designers. You tend to favor consistency. But
7 it seems --so bitcoin was one of the systems
8 that was opted.

9 So it's not a good thing or bad thing
10 per se. You need to understand -- I would say
11 it's good so long as the system behaves as you
12 intended.

13 Q. Okay.

14 A. Yes. So I wouldn't say it's good or
15 bad.

16 Q. Is safety necessary -- let me --
17 sorry. Let me rephrase.

18 Is it necessary for a decentralized
19 system to be safe?

20 A. The safety can be specified in
21 different ways.

22 So safety, yes, safety can be
23 specified in different ways. So it's important
24 that the safety is respected. Yes.

25 Q. I'm sorry. Are you saying that there

1 [REDACTED] - Highly Confidential

2 are different ways to understand safety?

3 A. Yeah. So safety is nothing bad.

4 Nothing bad happens. So for the specific

5 meaning, the specification of nothing bad

6 happens when you go and specify the system, this

7 would be different things.

8 Q. Okay.

9 A. So bad -- bad in bitcoin would be

10 that -- one thing. And bad in -- in some other

11 system would be something else. And they would

12 both be considered the safety properties.

13 Q. How does the safety of a system bear

14 on whether it is decentralized?

15 A. It does not.

16 Q. Does not. Okay. How do you measure

17 the safety of a blockchain system?

18 A. You measure it -- well, measure is

19 the -- there is a specification of safety. So

20 the system will need to specify what it intends

21 to do. What it tends to be done is split in

22 safety and liveness.

23 Q. Okay.

24 A. Roughly speaking, safety means nothing

25 bad will happen. And liveness means something

1 [REDACTED] - Highly Confidential

2 good will happen, so as you see the difference.

3 It's easy to design safe systems. They don't do
4 anything.

5 So that kind of by definition means
6 nothing bad will happen. So you will not have
7 force. You will not have whatever you can
8 imagine. But that's not a useful system.

9 And then you have the liveness
10 property that says, Okay, let's move on. Let's
11 do something. And this is where the two --

12 Q. Okay.

13 A. -- things come.

14 Q. Is your definition of liveness as
15 stipulating that good things eventually happen,
16 is that based on literature or your professors?
17 Or what is that based on?

18 A. Yes. Both. Both.

19 Q. Okay. What does it mean in your
20 definition of liveness on page 9 that good
21 things do eventually happen? What do you mean
22 by "eventually"?

23 A. This means typically that if the
24 system is let to be run for a very, very long
25 time, eventually means unboundedly long time,

1 [REDACTED] - Highly Confidential

2 but you still wait and you don't know how much
3 you will wait, but something will happen good,
4 so it doesn't stop and just cease to be
5 operational, right? That -- for eternity,
6 right? So that would be not live.

7 Q. So what is -- can you quantify
8 eventually? For a system to be -- for a system
9 to have liveness, what's the outer range of how
10 long someone would have to wait for a
11 transaction to go through --

12 A. There are systems that even --

13 MR. SYLVESTER: Wait to answer. Wait
14 for her to ask the question.

15 THE WITNESS: Yes. Sorry. Yes.

16 A. For some systems, they don't specify
17 role. Usually depends -- it relates to the
18 network. You remember we discussed this
19 unreliable network. We discussed asynchronous
20 network partition, forward network, et cetera.
21 So it's related to this concept. So when you
22 have a partition or unreliable network, it can
23 last for very long time. You're not going to
24 put a precise bound on that time.

25 Q. Okay. So your view is that a system

1 [REDACTED] - Highly Confidential

2 can be live with an unbounded degree of delay as
3 long as it eventually goes through?

4 A. That is the -- often the case -- so
5 liveness can be specified different. Liveness
6 of the system could be specified. The system
7 delivers a block every two seconds. You can
8 specify it like that, like good luck in this
9 world implementing that and maintaining that.

10 But it's usually, like, a relaxed
11 requirement in the system.

12 Q. Is there any scientific agreement on a
13 specific quantification of liveness?

14 A. So that --

15 MR. SYLVESTER: Objection.

16 A. There is agreement that it means, on a
17 high level, what I'm describing here. There are
18 different -- like, there are different --
19 different specification of safety. There are
20 different specifications of the liveness. And
21 this is totally normal, yes. You would still
22 call it liveness and safety, but they would mean
23 different things because they're attached to the
24 system that satisfies these properties.

25 Q. Can a centralized system have

1 [REDACTED] - Highly Confidential

2 liveness?

3 A. It can.

4 Q. So how does measuring liveness tell
5 you whether a system is it decentralized?

6 MR. SYLVESTER: Objection.

7 A. It doesn't. I didn't say it does. It
8 doesn't.

9 Q. Okay.

10 MR. SYLVESTER: Just pause for a
11 second for me to object.

12 THE WITNESS: Okay. Sorry.

13 MR. SYLVESTER: Thank you.

14 Q. Are there circumstances where by
15 design, a blockchain system prioritizes safety
16 over liveness?

17 A. There are.

18 Q. Can you give an example were?

19 A. Of a blockchain system?

20 Q. Yeah, that prioritizes safety over
21 liveness.

22 A. Since we discussed -- since we
23 admitted bitcoin Ethereum and XRP Ledger to be
24 blockchain systems, in this world, it's XRP
25 Ledger.

1 [REDACTED] - Highly Confidential

2 Q. XRP Ledger prioritizes safety over
3 liveness?

4 A. Yes.

5 Q. Why do you say that?

6 A. Because in the cases of network
7 partitions, it is designed to stop -- so, for
8 example, if you have a partition which splits
9 the network in two equal halves, XRP Ledger is
10 designed to stop making progress. So it would
11 wait for partition to heal, and two halves of
12 the network to start to communicate to each
13 other before you actually start that.

14 Q. Does prioritizing safety over liveness
15 mean that a blockchain is not resilient?

16 A. It does not mean that, no.

17 Q. Okay. I want to talk about the
18 Nakamoto coefficient, which you -- you reference
19 on page 9 of your report, as we discussed
20 earlier.

21 For the -- for the Nakamoto
22 coefficient, you cite to reference number 19 in
23 your report. What is that?

24 A. Again, for the -- the term, "Nakamoto
25 coefficient," not the meaning, I spent some time

1 [REDACTED] - Highly Confidential

2 explaining where does the -- in the sentence
3 before Nakamoto coefficient is introduced, I'm
4 saying, Scientific and engineering literature
5 uses this concept. So that's apart from calling
6 it Nakamoto coefficient. I'm calling it
7 Nakamoto coefficient for the purpose of
8 bettering the ability of the document. It comes
9 from Balaji Srinivasan, who is the ex-CTO of
10 Coinbase.

11 THE COURT REPORTER: I'm sorry. Comes
12 from what?

13 MS. ZORNBERG: I'll spell it.

14 THE WITNESS: Yes.

15 MS. ZORNBERG: First name,
16 B-A-L-A-J-I. Last name,
17 S-R-I-N-I-V-A-S-A-N.

18 A. Who was the ex-CTO of Coinbase, the
19 publicly listed exchange. And in that sense,
20 known figure in the space who used this term to
21 denote the -- what's important to focus on is
22 the definition of the notion that I'm trying to
23 capture, not -- so, again, we could call it
24 coefficient of Byzantine nodes, and this is my
25 motivation to call it that way. I'm citing

1 [REDACTED] - Highly Confidential

2 either his blog post or YouTube --

3 Q. Right.

4 A. -- video in which he explains it.

5 Yes.

6 Q. Okay. So, yeah, the -- the actual
7 reference in your report cites to the YouTube
8 video. Have you watched that YouTube video?

9 A. I did.

10 Q. When is the last time you watched it?

11 A. A few months ago. July, again.

12 Q. Have you also reviewed
13 Mr. Srinivasan's blog post on the same subject?

14 A. I -- I read that blog post, yes.

15 Q. Okay. Do you consider Mr. Srinivasan
16 an expert in blockchain systems?

17 A. I don't know if he was an expert or
18 not. I considered that he is a known figure in
19 the space.

20 Q. Did you consider the contents of his
21 video to be reliable?

22 MR. SYLVESTER: Objection.

23 A. Reliable? How did you define
24 "reliable"? The way we did few hours ago?

25 Q. That's fine.

1 [REDACTED] - Highly Confidential

2 A. Yes.

3 I think the -- the -- the notions that
4 he discussed in that video, to my recollection,
5 are pretty much reliable in a sense that, you
6 know, it's pretty clear what he talks about in
7 that blog post, yeah, or video.

8 Q. Have you ever spoken to Mr. Srinivasan
9 about his use of the term "Nakamoto
10 coefficient"?

11 A. No, I did not.

12 Q. Okay. Are you aware that the
13 presentation that Mr. Srinivasan gave in that
14 YouTube video was at the 2017 Blockstack Summit?

15 A. That sounds familiar, yes.

16 Q. Were you present?

17 A. No.

18 Q. Okay. So in the YouTube video,
19 Mr. Srinivasan begins by saying that
20 decentralization has not yet been quantified.

21 Do you recall that?

22 A. I don't recall word for word. I trust
23 you. Yes.

24 Q. I'll proffer to you that he says in
25 the video, quote, So everybody agrees that

1 [REDACTED] - Highly Confidential

2 decentralization is important. And the issue,
3 though, is it hasn't yet been quantified.

4 Closed quote.

5 A. That is possible. We're talking 2017.
6 For example, that seems to predate Troncoso
7 paper. As we see in the recent years, there is
8 more and more people. So if -- I don't know.
9 You mentioned Neha Narula. You mentioned this.
10 There is Balaji Srinivasan. I mentioned that.
11 And there is an ongoing interest. But this is
12 still 2017, and there is -- there are things
13 happening in between.

14 Q. Okay. So you're not disputing that as
15 of 2017, decentralization had not yet been
16 quantified.

17 MR. SYLVESTER: Objection.

18 A. Again, the quantified, we would need
19 to understand how you quantify, if you --
20 because discuss the measures or not -- what I
21 could tell is that -- that understanding that
22 I'm defending my report, which relates to the
23 papers that we discuss and the understanding,
24 that we, as a humanity and scientific community
25 and blockchain communities and call it whatever

1 [REDACTED] - Highly Confidential

2 you like. It advanced since 2017. So pulling
3 out -- I mean, not pulling out. Sorry. That's
4 not the right word.

5 Quoting sources from 2017 may not be
6 the right description of the -- of the situation
7 that we are currently facing in understanding
8 what decentralization is.

9 Q. How did Mr. Srinivasan derive the
10 Nakamoto coefficient in the system that he
11 presented in that presentation?

12 MR. SYLVESTER: Objection.

13 A. So my recollection of the -- of that
14 YouTube video, so he uses it in the way I define
15 it in this paper.

16 So this is the minimum number of
17 authorities that the adversary needs to control
18 in order to subvert key properties of the
19 system.

20 He looks at Nakamoto coefficient, a
21 different -- so most -- mostly he looks at
22 Nakamoto coefficient in the terms of mining
23 pools for bitcoin and Ethereum, which is what, I
24 guess, people are doing. And I did it in my
25 report, because we cannot -- it's really

1 [REDACTED] - Highly Confidential

2 difficult to understand.

3 Usually we assume that this Nakamoto
4 coefficient for these two networks is
5 considerably higher because the individual
6 mining tool does not control all the miners in
7 the pool. I could join one pool. I'm still
8 controlling my miners with some methods I could
9 detect if my mining pool -- my mining pool --
10 the mining pool that I'm contributing to is
11 trying to subvert some of the key properties of
12 the system. And if it happens, so I can decide
13 to leave that pool. So the assumption that the
14 pool operator -- the pool operators basically
15 take a fee -- like 2 percent, 4 percent is a
16 good ballpark. Don't quote me on this -- to
17 even rewards of miners over time. So
18 ordinarily, by joining the pool, you get less
19 rewards. But you get them more often, and more
20 evenly distributed, like. So --

21 Q. But --

22 A. Yes.

23 Q. I'm sorry. I think you've moved
24 beyond my question.

25 A. Perhaps I did, yes. You want to

1 [REDACTED] - Highly Confidential

2 repeat?

3 Q. Well, I'll just move on.

4 Is there agreement in the scientific
5 literature about how to measure the Nakamoto
6 coefficient of a blockchain system?

7 A. In the Nakamoto coefficient, so,
8 again, you use the Nakamoto coefficient the way
9 I use it in -- in the report. So as the minimum
10 number of authorities that the adversary needs
11 to compromise in order to subvert key properties
12 of the system, for the class of protocols that's
13 not proof of work, that's kind of easier.
14 Because you would always have a threshold of
15 faulty -- all XRP Ledger has it. It's not only
16 XRP Ledger. Other protocols that are -- belong,
17 let's call it, to this family of protocols have
18 that threshold.

19 It's easier to estimate this than, for
20 example, for proof of work. I was digressing a
21 moment ago, trying to explain the difficulties
22 of estimating that and proof of work. But
23 actually, in other consensus protocols, it may
24 be and it often is much easier.

25 Q. Do you know if everyone in the

1 [REDACTED] - Highly Confidential

2 scientific community uses the term "Nakamoto
3 coefficient" the same way you do in your report?

4 A. I'm pretty sure there are some
5 researchers who don't know about the exact term.
6 If we define it for them -- and this is what I
7 would -- you know, this is the essence of it.
8 Like, one should focus when it reads my report
9 on the definition, what it means.

10 And we can call it, you know, if we
11 can call it -- we'll call it [REDACTED] partition.
12 We can call it that way. If you want to call it
13 coefficient of Byzantine nodes, we can call it
14 that way. Or Nakamoto coefficient, we can call
15 it that way. That's less -- that's a handle
16 which we use to refer to the concept.

17 Q. Just for clarity, when you use
18 Nakamoto coefficient in your report, you're
19 using it as a shorthand for your own definition
20 that's provided in the sentence prior that you
21 read into the record.

22 A. No. I wouldn't agree fully. I --
23 it's not my definition. It's the definition
24 that I wrote in the report.

25 In that sense, it's my definition.

1 [REDACTED] - Highly Confidential

2 But it's not that I came up with it. As you
3 see, I'm writing about scientific and
4 engineering community has been using this for a
5 very long time.

6 Q. Okay.

7 MR. SYLVESTER: Lisa, we've been going
8 for about an hour, so whenever is a good
9 time to take a quick break.

10 MS. ZORNBERG: I would like to finish
11 on this -- on this note.

12 Q. Does Mr. Srinivasan derive his use of
13 the Nakamoto coefficient from the Lorenz curve
14 and the Gini coefficient?

15 A. He does not. He relates to them, but
16 he does not. So that's one of the points in the
17 Adriaens rebuttal that's misrepresenting the
18 facts.

19 Q. Okay. Let me show you Exhibit [REDACTED] 10.

20 MS. ZORNBERG: Mark, once we get
21 through this exhibit, we can take a break.

22 MR. SYLVESTER: Do you know about how
23 long it will be?

24 MS. ZORNBERG: I don't know.

25 Hopefully not too long.

1 [REDACTED] - Highly Confidential

2 MR. SYLVESTER: You let me know if
3 you're flagging and need a break.

4 THE WITNESS: I could use a break.

5 MR. SYLVESTER: Can we just take one
6 now, Lisa? He's saying he needs a break.

7 MS. ZORNBERG: That's fine.

8 MR. SYLVESTER: Thanks.

9 THE VIDEOGRAPHER: The time is
10 2:41 p.m. We're going off the record.

11 (Recess from 2:41 to 2:59.)

12 THE VIDEOGRAPHER: It is 2:59 p.m. We
13 are back on the record.

14 Q. Dr. [REDACTED] I've handed you
15 Exhibit [REDACTED] 10, which I'm going to represent to
16 you has -- shows two slides, from the video
17 presentation that Balaji Srinivasan gave called
18 quantifying decentralization that you cite in
19 your report.

20 Page 1 of the --

21 MR. SYLVESTER: Counsel, do you have
22 all the slides for context? Or just two
23 from the presentation?

24 MS. ZORNBERG: We have these two.

25 MR. SYLVESTER: Okay.

1 [REDACTED] - Highly Confidential

2 MS. ZORNBERG: I can't say for sure
3 whether they're the only two or not.

4 MR. SYLVESTER: Okay.

5 ("Quantifying Decentralization,"
6 Blockstack Summit 2017, was marked [REDACTED]
7 Exhibit 10 for identification, as of this
8 date.)

9 Q. Page -- the slide on page 1 of
10 Exhibit 10 is from four minutes in, and the
11 slide on page 2 of Exhibit 10 is from Minute 12
12 of the presentation.

13 So directing your attention to page 1
14 of Exhibit 10, the slide that Mr. Srinivasan
15 titled "Six Subsystems of the Bitcoin
16 Decentralized System."

17 Do you agree that those are subsystems
18 of the bitcoin blockchain system?

19 A. I do not.

20 Q. Okay. Why don't you agree?

21 A. Exchange is not a subsystem or a
22 bitcoin decentralized system.

23 It has nothing to do -- bitcoin
24 doesn't care if there is an exchange or not.

25 Q. Okay. Mr. Srinivasan also includes a

1 [REDACTED] - Highly Confidential

2 subsystem for nodes by country.

3 Do you agree that's a subsystem of the
4 bitcoin network?

5 A. I don't know necessarily what "nodes
6 by country" means here.

7 Q. Okay. Your report did not analyze
8 nodes by country for bitcoin Ethereum or
9 XRP Ledger, correct?

10 A. No. I'm referring to Srinivasan to
11 get a handle on the name of this concept.

12 Q. Okay. So you don't contend that
13 you're using Nakamoto coefficient in the same
14 way, necessarily, as Mr. Srinivasan.

15 A. I would say one of the users of
16 Nakamoto coefficient he has is the one that I'm
17 using it for. I'm not necessarily saying that
18 I'm using it in the -- all the -- I didn't go --
19 I didn't talk to the guy. I don't know the guy
20 personally. I don't know how he thinks about
21 it.

22 I saw the mapping. And I think it's
23 fair to say that this concept that I call
24 Nakamoto coefficient is sometimes called
25 Nakamoto coefficient because I'm pretty sure he

1 [REDACTED] - Highly Confidential

2 does it in that aspect. And that's where the
3 handle comes.

4 Q. Mr. Srinivasan roughly defined
5 Nakamoto coefficient during his presentation as,
6 quote, How many folks do you need to compromise
7 to get to 51 percent?

8 Closed quote.

9 Do you agree with that formulation?
10 Is that -- let me put it this way: Is that
11 formulation similar or different than the one
12 you use in your report?

13 A. You said how many guys.

14 Q. I'm quoting from him. How many folks
15 do you --

16 A. Folks.

17 Q. -- need to compromise to get to
18 51 percent?

19 A. I'm using it in a different way. So
20 I'm trying to make more -- to specify folks more
21 precisely. So we are talking about the
22 authorities that are contributing to the system
23 in some -- in some way, right? So they control
24 certain components of the system.

25 Q. What's an authority, as you use it, in

1 [REDACTED] - Highly Confidential

2 talking about Nakamoto coefficient?

3 A. I use it -- so authorities would be,
4 in the XRP Ledger, the organizations that run
5 the validator nodes.

6 Q. I'm sorry. Say it again.

7 A. The XRP Ledger, the organizations that
8 run the validator nodes. In the bitcoin
9 blockchain, the entities that run, we can say
10 full nodes or miner nodes. It depends. But you
11 can extend to full node.

12 If we say, for XRP Ledger, validators,
13 it would be only fair to talk about bitcoin full
14 nodes, so yes.

15 Q. Okay. So did I understand that if you
16 are going to do an apples-to-apples comparison
17 of XRP Ledger to bitcoin, the -- the right
18 comparison would be running a validator node on
19 XRP Ledger to running a full node on bitcoin or
20 Ethereum?

21 A. We need to define apples to apples,
22 but it's not the same. It's -- no. I didn't
23 say that. That's absolutely -- I didn't say
24 that.

25 I didn't mean that.

1 [REDACTED] - Highly Confidential

2 Q. So I'm just going to read back your
3 answer, make sure I understand what you are
4 saying.

5 What you previously said is, quote,
6 I'm sorry. Say it again. The XRP Company, the
7 organizations that run the validator nodes, in
8 the bitcoin blockchain, entities that run, we
9 can say full nodes or miner nodes. It depends.
10 But you can extend to full nodes. If we say for
11 XRP Ledger validators, it would only be fair to
12 talk about bitcoin full nodes. So yes.

13 Closed quote.

14 Explain -- it seems like you, as a
15 matter of fairness, were saying you should
16 compare XRP Ledger validators to bitcoin full
17 nodes.

18 Is that -- is that accurate?

19 MR. SYLVESTER: Objection.

20 A. I don't think it's accurate. We would
21 need to define "fairness."

22 Q. Well, what did you mean by that
23 statement? And if you want to correct it,
24 please do.

25 A. Yes.

1 [REDACTED] - Highly Confidential

2 There are certain similarities among
3 the -- but there is also deference, so it's not
4 apples-to-apples comparison. One would relate,
5 to a certain extent. And we can define
6 precisely how, XRP Ledger validators to bitcoin
7 full nodes.

8 It's not necessarily fair to call them
9 miners, miners, to relay them to miners, because
10 the miners get rewards for their engagement in
11 the bitcoin blockchain. Where actually,
12 validators on the XRP Ledger, they do not.

13 But then, again, it's not fully
14 correct to say that XRP Ledger validators are to
15 be thought of as full nodes on the bitcoin
16 blockchain. Because there is a certain security
17 aspect that, for example, if I'm running the
18 bitcoin full node validator and I'm running a --
19 a XRP Ledger validator which is not in the
20 main -- which is not in the dUNLs that we
21 discussed, there is a certain difference. So
22 the difference is mainly because in the XRP
23 Ledger -- shall I carry on?

24 Q. Not necessarily. No.

25 A. Okay --

1 [REDACTED] - Highly Confidential

2 Q. We can --

3 A. If you're happy --

4 Q. If you feel your answer is complete,
5 then --

6 A. No. If you -- you were unhappy with
7 my phrasing, so I'm trying to phrase. So if
8 you're happy, I can stop. If you're not happy,
9 I can continue.

10 Q. So my happiness is irrelevant as long
11 as you feel that you're giving accurate and
12 complete testimony.

13 A. I -- I -- you know, I am certainly. I
14 can continue discussing this. It's an
15 interesting point.

16 Q. Let me ask you a follow-up question.

17 A. Yes.

18 Q. And we'll go from there.

19 You mentioned that -- that miners get
20 rewards. Do -- do bitcoin participants who
21 operate nodes get rewards who are not miners?

22 A. Can you rephrase, please?

23 Q. Are there rewards in the bitcoin
24 system for validation?

25 A. There are no monetary rewards, like

1 [REDACTED] - Highly Confidential

2 there is monetary meaning in bitcoin token.

3 There are no rewards for that.

4 There are certain rewards. If you
5 think about contributing to the security of the
6 system, it's actually relevant. And there --
7 individually, I may get as a user who is
8 running -- not I. Whoever runs the bitcoin
9 validator node may get more privacy if he does
10 so in certain cases, which we can discuss.

11 Q. Okay.

12 A. So rewards in the terms of bitcoin
13 tokens, there are not.

14 Q. Okay. Let me direct your -- hold on.

15 You run a bitcoin node presently,
16 right?

17 A. I run a bitcoin full node presently.

18 Q. Do you receive any in-protocol
19 incentives for doing that?

20 A. In-protocol incentives? The way I --
21 the way I consider them in the -- in the report.

22 Q. Yeah.

23 A. No. So, no, no bitcoin is awarded for
24 running the validator.

25 Q. Okay. Let me direct you to the second

1 [REDACTED] - Highly Confidential

2 page of Exhibit 10, which, again, is a slide
3 that Mr. Srinivasan displayed during his
4 presentation, which you referred to in your
5 report.

6 According to this slide,
7 Mr. Srinivasan determined that both bitcoin and
8 Ethereum had a Nakamoto coefficient of 1.

9 Do you see that?

10 A. I see that.

11 Q. Do you know how he determined that the
12 Nakamoto coefficient for bitcoin was 1?

13 A. Looking at his columns, what he did is
14 that -- what I assume he did -- I cannot know
15 for sure -- what I'm assuming here that he did
16 is he took the minimum of the bitcoin column, so
17 basically mining says 5. Client says 1.

18 Developer says 5. Exchange says 5. Nodes says
19 171. Owner says 3. And similar for Ethereum,
20 this looks like taking the minimum out of these
21 columns.

22 Q. Okay. According to your report, if
23 the Nakamoto coefficient is 1, a system cannot
24 be deemed decentralized. Right?

25 A. Yes. I'm not saying what he did is

1 [REDACTED] - Highly Confidential

2 correct.

3 Q. Are you saying that what he did is
4 incorrect?

5 A. I would -- I would argue with him that
6 this is incorrect, yes.

7 Q. Why did you cite his YouTube video in
8 support -- as one of the 22 references your
9 report relies on if you thought his analysis of
10 Nakamoto coefficient was incorrect?

11 MR. SYLVESTER: Objection.

12 A. I'm using it in the way I cited it.

13 Q. Okay.

14 A. This notion is sometimes called
15 Nakamoto coefficient.

16 Q. Okay. Can I direct you to page 9 of
17 your report.

18 A. Yes.

19 Q. Besides Mr. Srinivasan's YouTube
20 video, do you cite any other authorities for the
21 term "Nakamoto coefficient" in your report?

22 A. I refer to the scientific literature
23 and engineering practice, which is -- I'm
24 reading this out verbatim again.

25 It's typically interested. And

1 [REDACTED] - Highly Confidential

2 herein, typically interested and scientific
3 engineering and literature engineering practice,
4 I am referring to my experience working on these
5 protocols for 18 years.

6 Q. Okay.

7 A. They're interested in the minimum
8 number of authorities that the adversary needs
9 to compromise to subvert the key property of the
10 system.

11 Again, we are getting into names.

12 Q. Okay. Understood. But my question
13 was really just a simple one. For your use of
14 the term "Nakamoto coefficient," does your
15 report cite to any authority other than
16 Mr. Srinivasan's YouTube video?

17 A. It refers to scientific literature,
18 engineering practice. If you want a citation in
19 the form that something concretely appears, it
20 does not.

21 Q. Okay.

22 A. But there is a reference to how people
23 approach these things.

24 Q. Okay. So Mr. Srinivasan's YouTube
25 video is the only citation for your use of the

1 [REDACTED] - Highly Confidential

2 term "Nakamoto coefficient," and Mr. Srinivasan
3 found Nakamoto coefficient of 1 for both bitcoin
4 and Ethereum?

5 MR. SYLVESTER: Objection.

6 Q. Correct?

7 A. It is not correct. So I'm saying that
8 this concept is sometimes referred to as the
9 Nakamoto coefficient. Implicitly, I'm referring
10 to scientific literature engineering practice
11 without explicitly pointing out to what I mean
12 here.

13 Q. Okay.

14 A. But there is a clear indication that
15 I'm referring to the larger body of literature,
16 which is not explicitly cited.

17 Q. What scientific literature are you
18 referring to?

19 A. This is a virtually all -- all
20 protocols that I have been working on for --
21 looking at it 18 years. So I have these
22 assumptions in my Ph.D. thesis. Leslie Lamport
23 has this notion that can relate to this in his
24 1980s paper. Miguel Castro and Barbara Liskov,
25 Turing Award winners, researchers at that time

1 [REDACTED] - Highly Confidential

2 at MIT who invented the PBFT protocol, have a
3 similar concept.

4 THE COURT REPORTER: Slow down,
5 please.

6 THE WITNESS: Yes.

7 A. So one can relate to these notions in
8 multiple scientific papers.

9 And these are called the threshold of
10 Byzantine nodes, threshold -- adversarial
11 threshold or similar names. We discussed this a
12 few hours ago.

13 Q. Okay.

14 A. I'm giving it a name, and it's just a
15 name.

16 Q. You talked about mining pools a little
17 while ago.

18 A. I did.

19 Q. In the bitcoin -- I have a clarifying
20 question.

21 In the bitcoin system, let's say that
22 Jeff controls Alice and Bob.

23 Does that count as one for the
24 Nakamoto coefficient as you're using it or as
25 three?

1 [REDACTED] - Highly Confidential

2 MR. SYLVESTER: Objection.

3 A. Can you repeat the question? How many
4 participants are there?

5 Q. Well, I -- there are three in my
6 hypothetical. So my hypothetical is Jeff
7 controls Alice and Bob in the mining pool.

8 A. Who is --

9 Q. Does that count as one or as three?

10 MR. SYLVESTER: Objection.

11 A. Who is Jeff?

12 Alice and Bob are running validator
13 nodes, but Jeff controls them. Jeff, mining
14 pool operator? Or --

15 Q. Yeah, let's assume he's a mining pool
16 operator.

17 A. What does it mean, controls? So
18 whatever Jeff decides, Alice and Bob implement?

19 Q. Yes.

20 A. It would be one.

21 Q. Okay.

22 Okay. Now, your report evaluates
23 bitcoin's resilience to the double-spend issue
24 and to the censorship-of-transactions issue.

25 Correct?

1 [REDACTED] - Highly Confidential

2 A. Correct.

3 Q. Are there any other elements to
4 resilience besides the double-spend and
5 censorship resistance that you're offering an
6 opinion about?

7 A. These are not elements of resilience.
8 Resilience applies to different -- to ensuring
9 different properties of the system. You just
10 mentioned the different properties of the
11 system.

12 Resilience would be, despite how many
13 Byzantine components of the system, do we still
14 reserve safety and liveness? So these are
15 not -- we discussed safety -- I think we
16 discussed this before. In safety, a measure of
17 resilience -- I'm -- I'm paraphrasing this,
18 but -- yeah.

19 Q. Okay.

20 So let's focus on double-spend. Why
21 is -- why is the issue of double-spend relevant
22 to decentralization?

23 A. I didn't write that it's relevant to
24 decentralization.

25 Q. Okay.

1 [REDACTED] - Highly Confidential

2 A. I wrote something else.

3 Q. Okay. Is it -- is it your opinion
4 that the double-spend issue is -- is a
5 separate -- separate and apart from whether a
6 system is decentralized?

7 A. Double-spend, the -- I'm giving it as
8 an example. If you read page 9, it says,
9 Informally, a safety property of a system
10 stipulates that bad things do not happen.

11 An example of a safety property, in
12 the context of blockchains, is double-spend
13 resistance.

14 Q. I understood. So double-spend and
15 censorship resistance are examples that you're
16 giving that relate to safety?

17 A. That is not fully correct. So
18 double-spend relates to safety. Censorship
19 resistance relates to liveness.

20 Q. Okay. So let's talk about
21 double-spend resistance.

22 What do you conclude with regard to
23 bitcoin's resilience to double-spend?

24 A. Just to find in the --

25 Q. I think it's on page 15 of your report

1 [REDACTED] - Highly Confidential

2 if you're looking for a reference.

3 A. Yes. Shall I read it out? I found
4 it.

5 Q. No. I don't need to you read it out.
6 Can you summarize, or can you just
7 point out --

8 A. Yes.

9 Q. -- where your conclusion is stated?

10 A. Let me -- let me read -- these two
11 paragraphs, and then I will summarize it if you
12 don't want me to read it out.

13 (Witness reviewing document.)

14 A. So I'm giving an example of how an
15 adversary which controls more than 50 percent of
16 the mining power, I'm giving high-level examples
17 what the adversary would need to do in order to
18 mount double-spending attacks and
19 transaction-censoring attacks. This is what I'm
20 doing in this paragraph.

21 Q. Okay. So -- so it's your opinion, as
22 expressed here, that more than 50 percent of
23 bitcoin mining power is controlled by four
24 mining pools. Correct? As of the date of your
25 report.

1 [REDACTED] - Highly Confidential

2 A. I'm not saying that. I'm saying that,
3 if we assume that the mining pool operator
4 controls -- and that's a big assumption. It's
5 not necessarily realistic.

6 If a mining pool controls all the
7 nodes in the mining pool, then four mining pools
8 control together 51 percent of the whole mining
9 power. Why is this not the case?

10 Q. Okay. Did you answer --

11 A. Yes.

12 Q. Let me direct you -- let me direct you
13 to the sentence on page 15, three-quarters down,
14 where you wrote, With this in mind, at the time
15 of writing this report, more than 50 percent of
16 bitcoin mining power is controlled by four
17 mining pools.

18 Do you see that?

19 A. I see that.

20 Q. You did not offer a citation in
21 support of that figure in your report. Right?

22 A. I did not. This is correct.

23 Q. Where did you derive your assertion
24 that as of October 4, 2021, more than 50 percent
25 of bitcoin mining power was controlled by four

1 [REDACTED] - Highly Confidential

2 mining pools?

3 A. I do not recall, unfortunately, the
4 sources precisely. I saw that number in -- I
5 verified it myself on certain websites that --
6 that indicate how much mining power is
7 controlled by which mining pool. Mining pool
8 often -- often identify themselves. When they
9 mine a block, they have -- some of them identify
10 themselves. It's possible to identify them.

11 Q. What websites did you rely on, in --
12 for that factual statement in your report?

13 A. I'm not saying this here. And I
14 don't -- I cannot quote from top of my head the
15 exact website. I also read, just to finish
16 my -- I didn't finish my response.

17 So there are also other scientific
18 papers that actually come to this number. So
19 that's -- it's not -- the moment that I looked
20 at it, at the moment I looked at it, I'm pretty
21 sure I looked at certain websites that track the
22 mining power, because the miners tend to, again,
23 identify themselves, some of them.

24 Q. Okay. But you don't remember -- you
25 make a statement that as of the writing of this

1 [REDACTED] - Highly Confidential

2 report, more than 50 percent of bitcoin mining
3 power is controlled by four mining pools. Is it
4 your testimony that for that figure, as of when
5 you wrote this report, you looked at websites
6 that you can no longer recall?

7 A. That I cannot recall from my head? If
8 I start searching, if I would be starting
9 searching it, I could probably tell you how got
10 it and why do I think this is -- this is
11 reliable.

12 Q. Why did you not identify those
13 websites, in your report, among the information
14 that you considered?

15 A. It was not my intention to hide any
16 information. You can call it an omission, if
17 you want, or oversight.

18 You can call it however you want. But
19 it was not my intention to note, Aha, I want to
20 give this information and hide this source.

21 I didn't think like that.

22 Q. How can we know if the websites that
23 you relied on for that factual statement are
24 reliable?

25 A. I -- did my best and honest work to at

1 [REDACTED] - Highly Confidential

2 think at that moment that they're reliable. So
3 they're not hidden websites. So reliable in a
4 sense that somebody could go, estimating, you
5 could probably get a historical -- you know, you
6 could go back and try to understand what I was
7 doing in July and August. So that would be
8 repeatable in a sense that we did find reliable.

9 And I think this is doable by an
10 independent researcher, to verify these claims.

11 Q. You agree that the percentage of
12 mining power that's controlled by mining pools
13 can change over time, correct?

14 A. I agree with that.

15 Q. It can change day to day, right?

16 A. It can change minute by minute if you
17 want, yes.

18 Q. Sitting here today, do you have any
19 basis to assert that the websites you recall
20 looking at, for that sentence of your report,
21 were reliable?

22 A. I have -- and this is not -- again
23 this is not the -- this is not the only source.
24 So there are scientific papers -- some of them
25 we -- I think we brought up today -- that

1 [REDACTED] - Highly Confidential

2 actually look at the same metrics, and they come
3 with the similar numbers.

4 So --

5 Q. And were those papers -- were there
6 any papers that you looked at that gave a
7 factual statement of the percentage of mining
8 power, controlled by mining pools, as of
9 October 4, 2021?

10 A. I would say, at that moment when I was
11 writing this, I had these papers in mind.
12 And -- but I was verifying this on these
13 websites, this information from these websites
14 that I was referring to.

15 Q. And you -- you agree it's an omission
16 in your report that you did not cite the
17 websites?

18 A. I --

19 MR. SYLVESTER: Objection.

20 A. -- said you can call it an omission.
21 I didn't say I agree. Yes. So it's something
22 that I didn't measure this for the first time
23 myself.

24 And like I didn't cite -- explicitly,
25 when I introduced the Nakamoto coefficient, I

1 [REDACTED] - Highly Confidential

2 didn't cite the body of literature. This is not
3 because I'm hiding references or something.

4 When I do this, it's mostly because I
5 think this is so easily verifiable that I almost
6 don't need to do it. This is my line of work,
7 rather than hiding information from anyone who
8 could be reading this report.

9 Q. Will you agree that if one mining pool
10 was in control of more than 50 percent of
11 bitcoin mining power, the -- the Nakamoto
12 coefficient for bitcoin would be 1?

13 A. I would agree that the very
14 conservative estimate as I write it in report,
15 under the assumption that a mining pool operator
16 authority controls all the nodes inside the
17 mining pool and only -- and under that
18 assumption, yes. Then yes.

19 Q. Okay. Has that occurred at any time
20 if bitcoin's history, to your knowledge? And by
21 that occurring, are you aware of any time in
22 bitcoin's history when one mining pool
23 controlled more than 50 percent of bitcoin
24 mining power?

25 A. I'm aware of certain -- certain --

1 [REDACTED] - Highly Confidential

2 I'll just point to -- not necessarily scientific
3 authors, maybe -- maybe even -- yes, I'm aware
4 that -- I suspect that in 2014, this occurred.

5 And, you know, you could arguably make
6 a statement in the very early days. We don't
7 know -- Satoshi Nakamoto is a group of
8 independent people or a single people, but you
9 could probably go back at the very beginning of
10 bitcoin blockchain and said -- make such a
11 claim.

12 So I'm aware of people making such a
13 claim. Again, one should be very careful.
14 There a big assumption about -- when we talk
15 about mining pools, so fast-forward to 2014 and
16 present days, there is this -- this is a very
17 conservative assumption in which you really
18 assume that the mining pool operator controls
19 all the nodes. This is normally not -- not
20 true.

21 Q. Okay.

22 MS. ZORNBERG: Can you show

23 Exhibit [REDACTED] 11.

24 (Article Dated June 16, 2014, "Bitcoin
25 Currency Could Have Been Destroyed by 51

1 [REDACTED] - Highly Confidential

2 Percent Attack," was marked [REDACTED] Exhibit 11
3 for identification, as of this date.)

4 MS. ZORNBERG: For the record,
5 Exhibit [REDACTED] 11 is an article dated June 16,
6 2014, called "Bitcoin Currency Could Have
7 Been Destroyed by 51 Percent Attack."

8 Q. Please take a moment to look at it.
9 But my question is, when you mentioned a moment
10 ago that you believed there was a time in 2014
11 when there was more than 50 percent
12 concentration of bitcoin's mining power, were
13 you referring to the incident that's described
14 in this article?

15 MR. SYLVESTER: Take a minute to read
16 the article if you haven't seen it before.

17 (Witness reviewing document.)

18 Q. Dr. [REDACTED] have you had a chance to
19 look at it?

20 A. I didn't finish, but I guess, you
21 know, we could -- just maybe just 30 seconds
22 more.

23 Q. Okay.

24 (Witness reviewing document.)

25 A. Yes, I had a chance to look at it.

1 [REDACTED] - Highly Confidential

2 Thank you.

3 Q. So is the 2014 incident described in
4 this article, when a mining pool called
5 GHash.io, spelled G-H-A-S-H.I-O, mining pool,
6 controlled more than 51 percent of the mining
7 power of bitcoin?

8 A. GHash.io, yeah.

9 Q. So let me just rephrase it cleanly.
10 When you talked about, earlier, a 2014 incident
11 when the mining pool concentration of bitcoin
12 exceeded 50 percent, were you referring to
13 the -- the GHash.io incident?

14 A. GHash.io. I believe this is the same
15 thing because I was talking about 2014. I'm
16 pretty sure that the -- it's very probable or
17 I'm pretty sure that I'm -- I was not looking at
18 the guardian document that you presented, but,
19 you know, different sources might have referred
20 to the same incident.

21 Q. Okay.

22 A. So, I believe it is fair to say I was
23 thinking of that. Yeah.

24 Q. So at the point of this 2014 incident,
25 would the Nakamoto coefficient of bitcoin have

1 [REDACTED] - Highly Confidential

2 been 1, according to your analysis?

3 A. According to my analysis, a very
4 conservative estimate of the Nakamoto
5 coefficient would be 1.

6 Q. Did it require human intervention to
7 avoid a threat in 2014 to bitcoin's safety and
8 liveness?

9 MR. SYLVESTER: Objection.

10 A. I couldn't know if it -- required
11 human intervention. It would be speculating for
12 me to understand if, you know, you could write a
13 software which immediately leaves the pool if,
14 you know, you are looking at something and you
15 says, Oh -- you could do it both ways.

16 Q. Okay. On page 2 of the article, the
17 writer of the article writes, quote, For the
18 brief period when GHash had 51 percent of the
19 network, the security of bitcoin wasn't a result
20 of its impressive mathematical background but
21 merely the trust that the users of GHash would
22 notice and respond if the pool's administrators
23 decided to try and abuse their position, close
24 quote.

25 Do you see that?

1 [REDACTED] - Highly Confidential

2 A. I lost you. Sorry. I apologize. I
3 lost you.

4 Q. It's the middle of page 2.

5 A. Middle of page 2.

6 For the brief period when GHash had
7 51 percent of the network, that paragraph?

8 Q. Yes.

9 And my question is, do you agree that
10 that's a fair statement?

11 MR. SYLVESTER: Objection.

12 Foundation.

13 A. This is a -- this is an article for
14 newspaper.

15 And I don't agree that the security of
16 bitcoin wasn't a result of its impressive
17 mathematical background, but merely the trust
18 that the users would notice and respond.

19 There is a -- there is an incentive
20 once you start playing this game, and I'm
21 referring to this in -- in my report. Once you
22 start playing this game of bitcoin, now assume
23 this happens -- let -- let's suppose that this
24 actually happened, and it happens today.

25 So now currently, you're controlling

1 [REDACTED] - Highly Confidential

2 51 percent of the mining power. Normally what
3 this means is that you are mining to get some
4 bitcoin rewards, and now you're facing the
5 dilemma, even if you could do it, is it good for
6 you.

7 If you are selfish, rational, economic
8 player, is it good for you to do it or not,
9 because you might -- you know, by mounting an
10 attack, you might be devaluing the trust in the
11 network, and that's actually integral part of
12 bitcoin, if you see what I mean.

13 So that dilemma that you are having,
14 even if you could somehow theoretically mount
15 the attack -- I don't know, U.S. governments
16 engages few nuclear power plants, starts mining
17 bitcoin, it gets to 51 percent. Now, does it
18 want to attack the network or does it want to
19 continue mining bitcoin because it's -- because
20 other -- you see what I mean.

21 So there is this part of the game
22 which is very difficult to say -- for example,
23 if the author says, The security of bitcoin
24 wasn't a result of its impressive mathematical
25 background. If I add game theory, game theory

1 [REDACTED] - Highly Confidential

2 is part of mathematics. That's a part of
3 bitcoin's background.

4 MR. SYLVESTER: You asked him if he
5 agreed. Let him finish.

6 A. Yes. So I could not agree with this.
7 It's a sensational article, and there are
8 certain challenges, of course, if you have
9 51 percent of the network, but there are
10 hidden -- not hidden aspects, there are actually
11 aspects of the whole game, theoretical
12 background of bitcoin, which is part of its
13 mathematical background, which actually puts you
14 in a dilemma of, when you're an attacker, Do I
15 want to do this or not.

16 Q. So are -- are you saying that someone
17 with 51 percent control might have incentives to
18 act in a trustworthy manner?

19 A. Yes.

20 Q. Okay.

21 Are you aware of any human activity,
22 in connection with the -- with the bitcoin
23 network, to prevent specific mining pools from
24 reaching 51 percent control?

25 A. I cannot comment on that. I don't

1 [REDACTED] - Highly Confidential

2 have any firsthand experience with it.

3 Q. Okay.

4 While we're on the topic of
5 double-spend, are you familiar with bitcoin
6 CVE-2018-17144?

7 A. I think this is -- I think I'm aware
8 of what you're discussing, yes.

9 Q. Okay.

10 What is a CVE?

11 A. I don't know exactly what CVE stands
12 for.

13 Q. Okay.

14 If I told you it stood for a common
15 vulnerabilities and exposure report, does that
16 sound familiar?

17 A. Fair enough.

18 Q. Okay. What do you recall of the -- of
19 the vulnerability that was at issue in
20 CVE-2018-17144?

21 A. To give you an objective precise
22 statement, I would need to refer to certain
23 documents.

24 What I recall from top of my head is
25 that there was a change in the bitcoin software

1 [REDACTED] - Highly Confidential

2 introduced in bitcoin core Version 0.14 to
3 optimize certain performance of the bitcoin
4 software.

5 Inadvertently or not, this change
6 we're introducing a vulnerability that -- that a
7 user could double -- to attempt to double-spend
8 the same inputs.

9 Because of the way bitcoin works,
10 you're spending certain outputs of a
11 transaction, so if you use the same input twice,
12 you're spending the -- if you're using the same
13 output of a previous transaction twice as the
14 input to your transaction, you're basically kind
15 of attempting to double-spend in some sense.

16 So like I have one bitcoin, but I
17 actually use it twice. So I'm kind of trying to
18 spend two bitcoins, and the vulnerability,
19 actually, was -- when it was first disclosed, it
20 was the -- that basically this would crash a
21 bitcoin 0.14, bitcoin core.

22 Q. Was a -- was a fix required to the
23 bitcoin software to resolve that issue?

24 A. Depends. So if you are running the
25 software before bitcoin Version 0.14, it was

1 [REDACTED] - Highly Confidential

2 not.

3 If you use -- because, you know, this
4 bug didn't exist -- if you call it a bug, this
5 didn't exist before 0.14. So if you ran a node
6 on 0. -- prior version to 0.14, you wouldn't be
7 required to change software, and it wouldn't
8 crash your machine.

9 Q. But if you were running the 0.4
10 version of bitcoin so that you had the bug in
11 your system, then you needed to download a -- a
12 fix to the bitcoin software.

13 A. You would need either to revert, as
14 you would not necessarily need to download.
15 There is a world in which you are reverting back
16 to a prior version of the code. Let's say you
17 have 0.13. On your machine you can install that
18 one.

19 Normally, this would -- so it's
20 reasonable to expect that more often than not,
21 this would -- for an operator of the node, this
22 would take some manual intervention. I could
23 imagine that you could write scripts if your
24 bitcoin machine starts failing, that it reverts
25 back to some previous item of the software, so

1 [REDACTED] - Highly Confidential

2 we cannot vouch that it would require human
3 intervention.

4 But it's possible that it would
5 require intervention of a human operator of a
6 node if it was running 0.14.

7 Q. Okay. So now I want to talk about
8 your analysis of censorship resistance in the
9 bitcoin system.

10 Are nodes required to accept all
11 proposed transactions into their block on the
12 bitcoin system?

13 A. What is a node?

14 Q. Do you know what a bitcoin node is?

15 A. I know, but like what are we talking
16 about here? So is it the bitcoin miner who gets
17 the transactions from the mempool. Is it the
18 validator node who gets the mine block and
19 validates transactions? What are we talking
20 about?

21 Q. Okay. I'm talking about a miner node.
22 Is a miner -- is a mining node required to
23 accept all proposed transactions into their
24 block?

25 A. A miner is free to decide on its own

1 [REDACTED] - Highly Confidential

2 which transactions it wants to include in the
3 block. It is incentivized by the bitcoin in
4 protocol incentives to essentially -- if it's a
5 rational economic player, it's incentivized to
6 select the transactions that carry the most
7 transaction fees.

8 Q. So, a miner can refuse to accept
9 transactions on the bitcoin network?

10 MR. SYLVESTER: Objection.

11 A. The miner could not opt to selectively
12 include certain transactions or not in the
13 blocks that it is mining.

14 Q. And -- and the miner can do that
15 unilaterally?

16 A. The miner can do that unilaterally --
17 it depends. If it joins the mining pool, then
18 somehow, sometimes the answer is no.

19 If the miner is independent miner,
20 it's fair to say that it can do it unilaterally.

21 Q. So if a mining pool can censor
22 transactions unilaterally, shouldn't that make
23 the bitcoins Nakamoto coefficient 1, under your
24 analysis?

25 MR. SYLVESTER: Objection.

1 [REDACTED] - Highly Confidential

2 A. No.

3 Q. Why not?

4 A. Because that's not correct.

5 Q. Why is it not correct?

6 A. It's not correct that if a mining pool
7 can opt which transactions to include, there are
8 other mining pools that can opt to include the
9 transaction.

10 So that wouldn't be censoring the
11 transaction, so if you want -- if the -- so what
12 you would get, effectively, is that the smaller
13 fraction, the smaller mining -- the complete
14 mining power that actually tries to include this
15 transaction in the blockchain is smaller than
16 100 percent.

17 And in principle, what it could do is
18 it could delay -- effectively it might delay a
19 transaction for a certain time.

20 In order to exclude the transaction,
21 as I write my report, to completely exclude the
22 transaction, or the longer period of time and to
23 mount the censorship attacks, we need to have
24 51 percent of the computing power of the cash
25 power in the network dedicated and really

1 [REDACTED] - Highly Confidential

2 committed to excluding this transaction, and
3 yes, they can do it; I mentioned it in my
4 report.

5 Q. So if a mining node on bitcoin can
6 unilaterally refuse to accept a transaction, are
7 you saying that transaction might have to be
8 resubmitted?

9 A. This is -- this is what's happening,
10 yes.

11 It depends, so I mean, you know, it
12 might never reach the -- yeah. I think --

13 Q. Okay.

14 A. -- I think it's clear.

15 Q. Let me direct you to page 9-- page 18
16 of your report.

17 Okay. And I'm turning now to your
18 analysis of Ethereum resilience.

19 So, on the -- that paragraph on
20 page 18, you make the statement, quote, At the
21 time of writing of this report, more than
22 50 percent of Ethereum mining power is
23 controlled by three mining pools, making the
24 conservative estimate of the Nakamoto
25 coefficient for Ethereum equal to 3, period,

1 [REDACTED] - Highly Confidential

2 close quote.

3 Do you see that?

4 A. I see that.

5 Q. You do not offer any citation for that
6 factual statement in your report, correct?

7 A. This is correct. And to explain that,
8 if I can expect your next question. Or you want
9 to pose it?

10 Q. I'd rather pose my questions --

11 A. Please.

12 Q. -- just since we're getting late in
13 the day.

14 A. Yes.

15 Q. Thank you, Doctor.

16 From where did you derive your
17 assertion that more than 50 percent of Ethereum
18 mining power is controlled by three mining pools
19 as of the writing of your report?

20 A. That would be the same approach that I
21 meant -- that I mentioned for bitcoin.

22 Q. Same websites?

23 A. It might be different websites. I --
24 I, unfortunately, cannot recall from top of my
25 head. It might be the same website which

1 [REDACTED] - Highly Confidential

2 aggregate information across different
3 blockchains.

4 Again, this is something -- so
5 these -- these websites usually -- you know, I
6 think this is verifiable because --

7 Q. Okay.

8 A. Yeah, I think this is verifiable.

9 Q. But --

10 A. Even -- even if I didn't give the --
11 that -- there are just many websites that do it.
12 There -- there are many researchers that --

13 Q. Okay.

14 A. -- came to similar conclusions, so
15 they use -- apparently science -- scientists use
16 this different information, and this information
17 is accessible.

18 I did my honest work to present this
19 honestly at the time of writing.

20 Q. Okay.

21 Let's turn -- by the way, would you
22 agree that it's -- as with bitcoin, for
23 Ethereum, it's possible for one mining pool to
24 control more than 50 percent of Ethereum's
25 mining power?

1 [REDACTED] - Highly Confidential

2 MR. SYLVESTER: Objection.

3 A. I would say we can relate to what we
4 discussed with bitcoin -- for bitcoin, and since
5 the consensus protocols are similar, I think it
6 would be fair to say that it's possible that a
7 single mining pool, on the Ethereum network,
8 controls more than 50 percent of the hash power.

9 Q. All right. Let's -- let's turn now to
10 your evaluation of the resilience of the XRP
11 Ledger, which you analyze on page 22 of your
12 report.

13 We looked at this earlier today. Is
14 the -- is the main conclusion or opinion offered
15 that the -- the existence of the dUNL, or a
16 dUNL, impairs the resilience of the XRP Ledger?

17 MR. SYLVESTER: Objection.

18 A. Can you repeat the question?

19 Q. Well, how would you state it? How
20 would you state -- what is your opinion about
21 the resilience of the XRP Ledger?

22 A. My opinion is -- of the XRP Ledger
23 resilience is that it doesn't tolerate single --
24 basically a single authority, being Byzantine,
25 and the single authority is the one that serves

1 [REDACTED] - Highly Confidential

2 in the release, 1.7.3, the dUNL.

3 I'm giving a simple example, but there
4 are other examples. I would like to point out
5 that this is not the only example of the attack
6 that could happen.

7 So, I'm describing later the other
8 possible -- some other possible attacks that may
9 happen from the untrusted validator list sites
10 that serves the d-- dUNL to the node.

11 Q. When you say "other examples," are you
12 referring to other examples in your report?

13 A. Yes.

14 Q. Okay. In your analysis of resilience
15 for the XRP Ledger, why did you not evaluate the
16 ledger's double-spend resistance in the way that
17 you did for bitcoin and Ethereum?

18 A. In a sense, I did.

19 So the -- the entire Section 4 of the
20 report.

21 Q. Okay. So please identify where --
22 where in your report you specifically evaluated
23 the double-spend resistance of the XRP Ledger.

24 A. For instance, and I will read -- I
25 will need to read in more details this section

1 [REDACTED] - Highly Confidential

2 to point you out to possible other examples.

3 But the double-spending is stated as a
4 challenge on page 20, in the first paragraph,
5 where I'm quoting the Chase/MacBrough paper, and
6 actually, when I say, Faces the same challenges
7 as other digital assets in preventing
8 double-spending and insuring network-wide
9 consensus, this is the citation from the Brad
10 Chase and Ethan MacBrough paper.

11 Q. So I --

12 A. -- I notice --

13 Q. I -- that -- that -- just to pause
14 there. So you're identifying that the
15 XRP Ledger, like other blockchain systems, have
16 to deal with double-spend and have to deal with
17 insuring network wide consensus. Right?

18 A. So, yeah, if you read this section,
19 I'm really putting my words in the brackets. So
20 I was trying to be careful here what are my
21 words and what I get from the sources that are
22 given by Ripple employees.

23 So whenever something is not in
24 brackets prefaced by my initials, this is what
25 I'm getting from one of the four sources that I

1 [REDACTED] - Highly Confidential

2 cite in Section 4.1.

3 Q. So my question is, where in your
4 report -- other than identifying that the
5 XRP Ledger has to face the double-spend issue,
6 where do you address how it does so?

7 A. For example, if you go to page 21.

8 And the second paragraph in
9 Section 4.1.2, "Consensus and Validation," the
10 second paragraph talks about the goal of the
11 XRP Ledger consensus protocol.

12 And then the third sentence --

13 Q. Well, where -- yeah.

14 A. -- or the second sentence, I say,
15 Roughly speaking, these properties are related
16 to double-spending prevention and censorship
17 resistance.

18 The following sentence, the third
19 sentence of the second paragraph of the
20 Section 4.1.2 says that, Formally, safety
21 properties relevant to XRP Ledger consensus
22 protocol are agreement in linearizability.

23 Q. Okay.

24 A. Quoting Chase/MacBrough paper, which
25 essentially mandates that correct validators

1 [REDACTED] - Highly Confidential

2 fully validate transactions in the same global
3 order, in the brackets, hence, preventing
4 double-spending.

5 From that moment on, when I talk about
6 safety properties of XRP Ledger, they are, at
7 this moment, tied to double-spending. And this
8 is the moment I establish the connection.

9 Q. Do you have an opinion that you're
10 offering in this case on the effectiveness of
11 the XRP Ledger in preventing double-spend?

12 A. I am offering the opinions of which
13 requirements -- what is necessary for XRP Ledger
14 to actually prevent double-spends.

15 I relied on the Chase/MacBrough paper.
16 I relied on my inspection of the critical parts
17 of the safety part of the consensus protocol.

18 I was also investigating whether this
19 part of the protocol changed since
20 Chase/MacBrough publish their paper, until the
21 point I was submitting my report. And this was
22 suggesting that -- this is -- basically this is
23 a valid understanding of -- of the protocol.

24 So --

25 Q. So --

1 [REDACTED] - Highly Confidential

2 A. -- if -- if the protocol -- if the
3 protocol prevents double-spending, there are
4 certain conditions under which it does so.

5 Q. Are you aware of a mechanism by which
6 a malicious actor can accomplish a double-spend
7 on the XRP Ledger?

8 A. I'm aware of certain mechanisms in
9 which this can happen, yes.

10 Q. What are those?

11 A. So, for example, if you look at my
12 report, page 21, this is fifth paragraph in
13 Section 4.1.2.

14 For two validators to agree on the
15 same global order of transactions, their UNLs
16 must intersect or overlap. Chase/MacBrough may
17 provide, in Section 4 of their paper, analysis
18 of the required UNL intersection across
19 different validators in order to guarantee
20 safety and liveness.

21 I read this, and I understood this
22 analysis, and I looked at the code to see their
23 changes with respect to this that would affect
24 the validity of the statement, because the paper
25 was in 2018, and then I looked at the key, for

1 [REDACTED] - Highly Confidential

2 example, quorum properties, et cetera. They
3 were unchanged from Chase/MacBrough.

4 And I support their conclusions. And
5 their conclusions say that the analysis in that
6 paper shows that to ensure safety of the
7 XRP Ledger consensus protocols, this requires
8 the intersection between any two UNLs to be over
9 60 percent.

10 Q. Okay.

11 A. Page 15 of that paper.

12 Q. Did you --

13 A. So there is a link to double-spending,
14 via safety.

15 Q. So what -- so -- did you say that you
16 reviewed what changes had been made to the
17 XRP Ledger protocol after the Chase/MacBrough
18 paper?

19 A. I did review. I was focusing on the
20 changes to the consensus protocol and trying to
21 see whether they would impact the analysis of
22 Chase and MacBrough.

23 I didn't -- I didn't find -- I found,
24 for example, that after the paper, the paper
25 assumes that -- for example, for liveness, it

1 [REDACTED] - Highly Confidential

2 assumes 80 percent quorums.

3 And there was a -- after the paper was
4 published in 2018, there was a change to the
5 XRP Ledger consensus protocol because, to my
6 recollection, the assumed size of the core was
7 67 percent of two-third majority in the code,
8 and it was supposed to be 80.

9 So there was -- there were codes
10 changes that were going towards fulfilling the
11 assumptions of operations that Chase and
12 MacBrough had in their paper; this -- this
13 occurred, but there were none that would affect
14 the analysis.

15 I'm pointing out, we discussed
16 negative UNL briefly. Negative UNL would affect
17 their analysis. It would not necessarily
18 undermine my conclusions, but it would affect
19 Chase and MacBrough analysis, but this change
20 was not effective at the time I was writing the
21 report and at the time -- for the release that I
22 looked at.

23 Q. Okay.

24 MS. ZORNBERG: I'd like to take a
25 break. I need a break, actually. So can

1 [REDACTED] - Highly Confidential

2 we go off the record.

3 THE VIDEOGRAPHER: The time is
4 3:53 p.m. We're going off the record.

5 (Recess from 3:53 to 4:13.)

6 THE VIDEOGRAPHER: It is 4:13 p.m. We
7 are back on the record.

8 Q. Okay. Dr. [REDACTED] can I direct you,
9 please, to page 16 of your report.

10 And this is part of your discussion of
11 governance for bitcoin.

12 I want to direct you to the first
13 two lines under "Governance," where you wrote,
14 Concerning code improvement proposals, anyone
15 can propose a change to the bitcoin open source
16 software via a bitcoin improvement proposals.
17 In practice, relatively few core developers,
18 developers of the bitcoin core reference node
19 software, propose and implement changes.

20 Do you see that?

21 A. I see that.

22 Q. In your view, is the fact of -- that
23 there are relatively few core developers on the
24 bitcoin system -- hold on, I have to rephrase.

25 Does the fact that rel-- that there

1 [REDACTED] - Highly Confidential

2 are relatively few core developers on the
3 bitcoin system mean that the bitcoin network is
4 centralized?

5 A. This is not what I mean, no. I
6 wouldn't support that claim.

7 Q. So in your view, bitcoin is
8 decentralized, notwithstanding the fact that it
9 has relatively few core developers?

10 MR. SYLVESTER: Objection.

11 Q. You can answer.

12 A. I'm writing, In practice, relatively
13 few core developers propose and implement
14 changes.

15 I stand by the opinion expressed in my
16 report that bitcoin is decentralized, so we can
17 say that this doesn't make -- the relatively few
18 core developers proposing and implementing
19 changes to bitcoin is not preventing me to --
20 under my methodology, to say that bitcoin is
21 decentralized.

22 Q. Okay.

23 Do you believe that bitcoin is the
24 only digital asset that will be needed in the
25 future?

1 [REDACTED] - Highly Confidential

2 MR. SYLVESTER: Objection. Beyond the
3 scope.

4 A. I don't necessarily have that belief.

5 Q. Do you believe that other digital
6 assets are inferior to bitcoin?

7 MR. SYLVESTER: Objection. Beyond the
8 scope.

9 A. Can we define "inferior"?

10 So I can answer the question.

11 Q. Have you publicly expressed the view
12 that bitcoin is superior to other digital
13 currencies?

14 A. I don't believe that I expressed my
15 view that it's superior to other digital
16 currencies.

17 If I did, please point me to the place
18 where I have -- did that. I don't believe I
19 did.

20 Q. Do you believe that bitcoin will
21 become the dominant form of money on earth?

22 MR. SYLVESTER: Objection. Beyond the
23 scope.

24 A. I believe that there would be good
25 things that would happen if this is so.

1 [REDACTED] - Highly Confidential

2 One cannot necessarily predict the
3 future.

4 Q. So would you want bitcoin to become
5 the dominant form of money on earth?

6 MR. SYLVESTER: Objection.

7 A. I think it would be -- it has good
8 connotations, so I think it would be better
9 for -- I -- I think it would be good for all of
10 us, as a humankind, to have common money that is
11 sound and that cannot be necessarily -- that
12 would have better properties than the money that
13 we have today.

14 To my understanding, bitcoin fulfills
15 this, and it's a very good candidate, if it
16 becomes dominant money, that it brings good to
17 all of us, regardless of the current
18 understanding of each and every one of us about
19 bitcoin.

20 Q. You -- you argued in your position
21 paper, in [REDACTED], that bitcoin's power
22 consumption is not wasteful or excessive.
23 Correct?

24 A. I argued in the paper that you
25 submitted that -- as Exhibit --

1 [REDACTED] - Highly Confidential

2 Q. Exhibit 5.

3 A. -- [REDACTED] 5?

4 Q. Yes.

5 A. [REDACTED] 5. I argued for that, yes.

6 Q. Are you concerned about the -- the
7 impact that bitcoin's energy consumption has on
8 the environment?

9 MR. SYLVESTER: Objection. Beyond the
10 scope.

11 A. Let me put it this way, so when I
12 think about it, as I mentioned in my paper, the
13 data I was able to obtain suggested that bitcoin
14 has zero -- consumes 0.1 percent of the total
15 world's energy production.

16 At that stage, to blame, currently,
17 bitcoin for climate change and other things is a
18 far-fetched thing. Like what happens to other
19 99.9 energy? So to blame it at this moment is
20 not -- is, to my understanding, not justified.

21 Q. Do you -- do you think that energy
22 consumption contributes to climate change?

23 MR. SYLVESTER: Objection. Beyond the
24 scope.

25 A. I don't have understanding to that. I

1 [REDACTED] - Highly Confidential

2 don't have deep understanding to that, yeah.

3 Q. Let me direct your attention to
4 page [REDACTED] of [REDACTED] Exhibit 5.

5 And I'll -- I'm just going to read
6 into the record the paragraph in the middle of
7 that page, where you wrote, quote, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

15 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

25 Did you write that paragraph?

1 [REDACTED] - Highly Confidential

2 A. I wrote this paragraph.

3 Q. Okay. And as you sit here today, does
4 that express a view that you hold?

5 A. I am here so the paragraph that you
6 read is the closing paragraph of [REDACTED]
[REDACTED]

8 And it -- for the record, because we
9 are taking this out of the context, is the --
10 argument tries to -- so I'm trying to argue that
11 if you have an inflationary money, that people
12 are not incentivized to save, they're
13 incentivized to spend. This is the part that we
14 skipped.

15 As people are incentivized to spend,
16 and they either spend money, they consume
17 things, they consume products, et cetera, or
18 they invest money into businesses and different
19 sort of things, as we know, so I'm just
20 summarizing other parts of --

21 Q. I don't -- I want you to complete your
22 answer --

23 A. Yes.

24 Q. -- but I don't need you to do
25 extensive summaries. My -- my question was just

1 [REDACTED] - Highly Confidential

2 whether that paragraph expresses your view as
3 you sit here today.

4 A. I --

5 MR. SYLVESTER: Objection.

6 A. Yes, so I think it's important to say
7 the view on what, essentially? The view on?

8 Q. Have you retracted anything in the
9 paragraph that I read on page [REDACTED] since
10 publishing it?

11 A. Rereading it, I don't find anything
12 that I would retract.

13 Q. Okay. Can I -- can I ask you to turn
14 to page [REDACTED] of Exhibit 5.

15 And in the -- you state that in this
16 position paper, quote, [REDACTED]
[REDACTED]
[REDACTED]

19 Do you see that?

20 A. I see that.

21 Q. Okay. And "we" means you.

22 A. I, yes.

23 Q. Okay.

24 On page [REDACTED] of the article -- of your
25 position paper, you -- you write, and this is

1 [REDACTED] - Highly Confidential

2 part of the last sentence on the top half, that,

3 [REDACTED]

8 Is -- is that [REDACTED] project one

9 that you're working on currently?

10 A. I'm referring to the [REDACTED] project
11 that I'm contributing to in some sense --

12 Q. Okay.

13 A. -- today, yeah.

14 Q. Do you -- do you receive compensation
15 for contributing to that project? For [REDACTED]

16 A. I do. Yes.

17 Q. Okay. On page [REDACTED] of your position
18 paper, in the middle of the page, you -- you
19 talk about tokens that have a genuine use case.
20 Is the only example that you cite there,
21 bitcoin?

22 A. I'm doing e.g., so this is example.

23 Q. Okay.

24 A. There might be others, so the example
25 that I'm giving is bitcoin.

1 [REDACTED] - Highly Confidential

2 Q. And that's the only example you
3 specifically give there?

4 A. That's the only example I specifically
5 gave in that sentence.

6 Q. Okay. Let me ask you to turn to
7 page [REDACTED] of Exhibit 5. About three-quarters of
8 the way down, I want to read a sentence that you
9 wrote, quote, Author's -- wait, I want to --
10 okay, I'll read the quote now that you're there.

11 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

15 Can you describe what you mean by
16 [REDACTED]?

17 MR. SYLVESTER: Objection.

18 Go ahead.

19 A. Yes. So I mean, something that -- I
20 was looking into bitcoin for 11 years. I
21 understood it well, to my understanding, as a
22 computer science system.

23 And I understood that it gives people
24 control over money and everything, but this is
25 not necessarily changing the whole behavior of

1 [REDACTED] - Highly Confidential

2 us as -- as human beings, as a species, to which
3 I'm referring in the -- in the paragraph that --
4 that you -- that you read previously.

5 So that -- to go to that
6 understanding, you're -- you need -- one needs
7 to -- in my opinion, one needs to step out from
8 looking at bitcoin as a computer science system,
9 as a transaction processing system.

10 So one would actually need to, in my
11 opinion again, look at bitcoin like
12 implications, what is it use case. In this
13 paper I'm discussing what is the use case.

14 I'm saying if it's a payment system,
15 well, spending 0.1 percent of world energy on a
16 payment system hardly is justified, but let's
17 try to understand what it does.

18 And as we are trying to understand
19 what it's doing, let's imagine -- so, okay, this
20 idea, it seems that its goal is to become the
21 money that we all use on this planet. So now
22 you are saying, But it spends that much energy.

23 So, now you need to understand, Okay,
24 but what do I get? If this is the money of the
25 future, what would I get in such a world.

1 [REDACTED] - Highly Confidential

2 And now you're starting to think, and
3 I realize, I explained to myself, that
4 essentially incentives of humankind change, and
5 it will make -- it will bring us, and this is
6 what I'm arguing in the paper, to save
7 resources.

8 To save. It just orients, instead of
9 spending, and as I say, I -- I don't think
10 it's -- I just think it's a technological
11 evolution. It's not -- even if one had an idea
12 such as to implement such a monetary policy,
13 this was practically impossible. The technology
14 was missing.

15 So, you know, in the history money,
16 there are like -- everybody -- always somebody
17 would come and be able to inflate the money
18 regardless of how we did it.

19 And now we have a tool which we could
20 use to actually promote savings and not
21 overconsumption of resources. I'm trying --

22 Q. And that's bitcoin?

23 A. I'm trying to convey this message, and
24 bitcoin, with its security and with the
25 predictable monetary policy, which basically

1 [REDACTED] - Highly Confidential

2 incentivizes savings, it's going in the
3 direction.

4 Q. Okay.

5 A. So once I realized that -- you asked
6 me about [REDACTED] Once I realized that, I
7 realized, Okay, this is -- as a computer science
8 system, this is -- this is a nice protocol. I
9 mean, it's interesting. It's consensus. It's
10 interesting because I was looking into that from
11 my professional standpoint.

12 But, you know, in -- in terms of my
13 talks, I would say, bitcoin spends lot of
14 energy. And usually when you do that, it's
15 because of the number of transactions per second
16 it processes, relatively high latency, and you
17 consider it is a transaction processing system,
18 as a payment system.

19 But once you understand that this is
20 not necessarily the use cases -- actually, use
21 case could be something else -- then you go back
22 and say, Okay, do -- is it reasonable to devote
23 energy of humankind towards that?

24 Q. Okay.

25 Did your enlightenment about bitcoin

1 [REDACTED] - Highly Confidential

2 come around the same time as [REDACTED]
[REDACTED]

4 MR. SYLVESTER: Objection.

5 A. Is that really relevant? So, I -- I
6 spent before -- let's put it this way. [REDACTED]
[REDACTED]
[REDACTED]

9 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

13 Q. Okay. Now, in your -- both in your
14 report and in your position paper, you talk
15 about the fact that if Ethereum moves from proof
16 of work to proof of stake, that will affect its
17 level of decentralization. Correct?

18 A. This is correct. It might affect the
19 level of decentralization.

20 So, I can elaborate on that if you
21 wish.

22 Q. Well, my question is, in your view, is
23 there any way for a proof-of-stake system to be
24 decentralized?

25 A. There is a way. We discussed one

1 [REDACTED] - Highly Confidential

2 idea. There is a way, so if we take a snapshot
3 of time, we apply Troncoso definition. We
4 cannot find a single authority that controls the
5 system.

6 And it is possible that this is the
7 case. There just -- I would say, in our
8 spectrum of the systems which pass from causal
9 definition, and if you apply inclusiveness or if
10 you value more permissionless system than
11 permissioned or -- or inclusive as opposed to
12 noninclusive, then it would put proof of stake
13 on a -- less decentralized than bitcoin.

14 Plus there is this danger, which I
15 don't elaborate in the report -- is that
16 whenever you have the -- I think one example is,
17 for example, you know, in any -- in any
18 industry, how bigger players, over the time, do
19 mergers and acquisitions of smaller players, et
20 cetera. Right?

21 So there is this danger that the power
22 in the system concentrates. For example, if I'm
23 controlling 30 percent of the stake, depending
24 on how the stake game is set, how the incentives
25 are set, I might get more and more and more

1 [REDACTED] - Highly Confidential

2 tokens, and if you're not careful when you
3 design this system, you know, as the power of
4 such a stake grows, you could go over
5 50 percent.

6 So, you know, it's -- it's more -- in
7 my opinion, there is more tendency for a system
8 based on proof of stake, more challenges to keep
9 it decentralized than it's -- it is for proof of
10 work.

11 Q. Okay.

12 Let me direct you to page 25 of your
13 report. I'm moving to another topic.

14 And -- and this is a page of your
15 report where you are responding to Question E2.

16 Do you see that?

17 A. I see.

18 Q. And we -- we talked about Question E2
19 this morning. And you noted that you might have
20 to rethink this section of your opinion, based
21 on recent changes to Ripple D. Correct?

22 A. In the context of --

23 MR. SYLVESTER: Objection.

24 Go ahead.

25 A. Yes. In the context of my report, if

1 [REDACTED] - Highly Confidential

2 it's fixed in time and it looks at one point,
3 7.3, the answer would be no.

4 If someone -- if the Court, SEC,
5 whoever, asks me to opine and I accept to do
6 that on one -- if you -- so if one would allow
7 it 1.8.1, we would need to revise this section.
8 Yes.

9 Q. Okay. So I want to direct your
10 attention to Number 1 in your -- in -- in your
11 answer to Question E2, where you talk about
12 things Ripple does or has done. And you -- you
13 quote a Ripple employee named Nick Bougalis.

14 Do you see that in the second
15 paragraph?

16 A. I see.

17 Q. Do you know Nick Bougalis?

18 A. I don't know him.

19 Q. Okay. And you -- you state that in an
20 XRP chat online, in October 2020, from a user
21 who appears to be Ripple's employee Nick
22 Bougalis, following a November 2018 incident,
23 he, quote, personally restarted several
24 validators, close quote.

25 Do you see that?

1 [REDACTED] - Highly Confidential

2 A. I see that.

3 Q. Okay. I want to show you

4 Exhibit [REDACTED] 16.

5 (XRP chat was marked [REDACTED] Exhibit 16 for
6 identification, as of this date.)

7 Q. You're welcome to take a look, of
8 course, through the whole document. I will
9 point out that, you know, this is -- this is the
10 XRP chat you appear to quote, and the section
11 you appear to quote is on the third page of the
12 document. And that's the only page I'm going to
13 ask you about.

14 A. Yes.

15 Q. Do you agree that Exhibit 16 is the
16 XRP chat you were referring to on page 25 of
17 your report?

18 A. I believe I can agree with that.

19 Q. Okay. Can you look about midway down
20 Exhibit -- page 3 of Exhibit 16, and starting
21 with the place in the chat where Mr. Bougalis
22 wrote, I personally restarted, and compare it to
23 the quote that you excerpted in your report, and
24 tell me if you think that you've accurately
25 quoted the chat.

1 [REDACTED] - Highly Confidential

2 MR. SYLVESTER: Objection.

3 (Witness reviewing document.)

4 A. So under "Quotations" in my report, I
5 attributed that Nick Bougalis, following the
6 November 2018 incident, he personally restarted
7 several validators.

8 If I look at the document, it says I
9 personally started several of Ripple's
10 validators.

11 Q. That's a difference. Right?

12 A. There is a --

13 MR. SYLVESTER: Objection.

14 Go ahead.

15 A. There is a difference in a sense that
16 I skipped that he restart, so in the quotation
17 marks, I skipped that he restarted Ripple's
18 validators.

19 Q. Okay. And -- and do you agree that
20 the actual sentence in the XRP chat in
21 Exhibit 16 reads, quote, I personally started
22 several of Ripple's validators, and other
23 validator operators restarted theirs, period,
24 close quote?

25 MR. SYLVESTER: Objection.

1 [REDACTED] - Highly Confidential

2 A. I believe I -- you said I personally
3 started where it's written I personally
4 restarted, several of Ripple's validators.

5 Q. Okay. Dr. [REDACTED] have I -- do you
6 agree that I've correctly read from M 16 that
7 the statement in the chat was, quote, I
8 personally restarted several of Ripple's
9 validators, comma, and other validator operators
10 restarted theirs, period, close quote?

11 Did I read that correctly?

12 A. You read that correctly. I just
13 corrected you because I heard that you said I
14 personally started.

15 Q. Okay.

16 A. Yeah.

17 Q. In your report you -- you left out, Of
18 Ripple's validators. You -- you wrote, quote,
19 He personally started several validators, close
20 quote.

21 So you left out two things. Right?
22 You left out that he actually stated that he had
23 restarted several of Ripple's validators, and
24 you also omitted the part of the sentence
25 stating that other validators restarted theirs.

1 [REDACTED] - Highly Confidential

2 MR. SYLVESTER: Objection.

3 Q. Correct?

4 MR. SYLVESTER: Objection.

5 A. I did not -- I did not omit. I was
6 taking the part of the sentence on the quotation
7 marks since what we could agree is that I didn't
8 put -- attribute that validators are Ripple's
9 validators.

10 Q. Okay. So do you agree that your
11 report inaccurately quotes Mr. Bougalis in -- in
12 that XRP chat?

13 MR. SYLVESTER: Objection.

14 A. I would say that it's -- apparently
15 doesn't quote it word for word. If you
16 restarted several validators, you -- if you
17 restarted several Ripple's validators, you
18 restarted several validators, so it's not
19 incorrect.

20 As for use of quotation marks, if they
21 are meant to mean exactly what was written,
22 there is missing "of Ripple's validators." So
23 there should be "several of Ripple's
24 validators."

25 I -- I can explain the -- the context

1 [REDACTED] - Highly Confidential

2 if you wish.

3 Q. No.

4 A. No? Okay. No.

5 Q. Given the accurate quote from

6 Mr. Bougalis, what is your basis for saying that

7 in particular, Ripple's -- Ripple employees'

8 effort was needed?

9 A. So, we didn't focus on the second --

10 so you basically added -- I was asked, so

11 let's -- let's roll back to the question, E2; to

12 what extent have Ripple's efforts been needed to

13 support the proper function of XRP Ledger.

14 I'm trying to answer that question.

15 This doesn't mean that there are no other's

16 efforts involved in this. I'm trying to answer

17 whether the Ripple's efforts be needed to

18 support the proper functioning of XRP Ledger.

19 When I'm jumping to -- when -- when

20 you're jumping, illustrating, in particular,

21 Ripple's employees, we should also focus on the

22 second sentence, which I believe is quoted,

23 Without differences.

24 So the team at Ripple invested a

25 significant amount of time troubleshooting the

1 [REDACTED] - Highly Confidential

2 issue and proposed several improvements.

3 This looks word for word.

4 Now, illustrating the amount of human
5 and, in particular, Ripple, so the quotations
6 that I'm giving are, in particular, illustrating
7 the amount of effort of Ripple's employees.

8 Q. Dr. [REDACTED] I'm not questioning the
9 second quotation, just so you know.

10 It's only the first quotation where
11 I -- I wanted to point out, and you've
12 acknowledged, that there are missing words from
13 within the quotation marks.

14 A. Yes, I believe, if I'm not mistaken,
15 that you asked me about the conclusion that, in
16 particular, Ripple's employees' efforts are
17 needed, so this is why I'm pointing out the
18 second.

19 For the first one, I think we are in
20 agreement.

21 Q. Okay. Let's turn to Question E3 in
22 your report where you were asked, on the bottom
23 of page 25, quote, What risks to the XRP Ledger
24 would or might materialize if Ripple walked away
25 or disappeared? Do you see that?

1 [REDACTED] - Highly Confidential

2 A. I see that.

3 Q. Was that a hypothetical question given
4 to you?

5 A. That was a question giving -- given to
6 me for an opinion as -- as it was phrased here,
7 so I didn't come up with a question. I was
8 given that question to answer it.

9 Q. Okay.

10 And you answer it at the bottom of
11 page 25 by saying that, Serious risks may arise.
12 Correct?

13 A. They may arise. We don't -- yes.
14 This is what I said.

15 Q. So "may" means maybe they would, maybe
16 they wouldn't?

17 MR. SYLVESTER: Objection.

18 A. May arise, it's -- there is a
19 possibility that they may arise.

20 Q. Is it fair to say you're not providing
21 an opinion in response to Question E3 about what
22 will happen to the XRP Ledger if Ripple
23 disappeared?

24 A. I'm not providing answer to that
25 question, because it was not a question.

1 [REDACTED] - Highly Confidential

2 Q. Okay. In answering the question in
3 E3, does your report cite to any scientific
4 literature?

5 A. No, it does not. I'm answering my
6 question to the best of my understanding of the
7 protocol.

8 Q. Okay. So, it looks like you -- you --
9 in answering the question, you posited
10 two possible cases, Case A and Case B.
11 Do you see that on page 26?

12 A. I see.

13 Q. So in Case A, you considered what
14 might happen if Ripple disappears and the
15 network is still able to agree on the contents
16 of the dUNL as currently published on
17 VL.Ripple.com. Correct?

18 A. This is correct.

19 Q. And -- and you conclude that in the
20 case where more than 20 percent of the
21 validators in the dUNL disappear, the network
22 would not be operational. Right?

23 A. I agree.

24 Q. Okay. And you -- given the -- you do
25 a calculation that because there are -- you

1 [REDACTED] - Highly Confidential

2 calculate 41 total entities on the dUNL, as of
3 October 4, 2021, you say that, hence, the
4 network would cease to be operational if nine
5 validators disappeared, right?

6 A. 20 percent of 4.1 being 8.2, rounded
7 up, so this means that the network would
8 continue to provide liveness, and be operational
9 in that sense, with 8 disappearing validators,
10 it would take 9 to halt the network.

11 Q. Does your conclusion assume that the
12 XRP Ledger network consists solely of validators
13 using the unmodified dUNL?

14 MR. SYLVESTER: Objection.

15 Go ahead.

16 A. So, we considered two cases as I write
17 on page 26. Ripple disappears, and the
18 assumption for the analysis is that the network
19 is still able to agree on the contents of the
20 dUNL as nan currently published on
21 <https://VL.Ripple.com>.

22 So that happens, we are dealing with
23 the network in this imaginary example, right,
24 what might materialize? I'm assuming that the
25 dUNL is the same.

1 [REDACTED] - Highly Confidential

2 Q. So my question was, does your scenario
3 or Case A also assume that the XRP Ledger
4 network consists solely of validators using the
5 unmodified dUNL?

6 MR. SYLVESTER: Objection.

7 A. As I mentioned, it assumes that the
8 network is able to agree on the contents of the
9 dUNL as currently published there, so what I'm
10 discussing is the case -- what I'm considering
11 is the case where the dUNL is the same as
12 currently published on VL.Ripple.com.

13 Q. Do you know, as of October 4, 2021,
14 how many validators on the system use the
15 unmodified dUNL?

16 A. I don't know.

17 Q. You don't know by percentage or by
18 total?

19 A. I don't know.

20 Q. Did you do any work in this case to
21 try to determine how many validators use the
22 unmodified dUNL?

23 A. That would probably necessitate that
24 there is a disclosure of that by natural
25 cooperators, the answer would probably be no.

1 [REDACTED] - Highly Confidential

2 Q. So you're not even sure it's knowable?

3 A. It's know--

4 MR. SYLVESTER: Objection.

5 A. It's knowable -- it's knowable in a
6 sense that -- from the God's perspective it's
7 knowable. If we interview all the node -- all
8 the node operators and they're honest, they tell
9 us the truth, it's knowable.

10 Q. Okay. You didn't do that?

11 A. I didn't do that.

12 Q. Okay. How many validators were active
13 in the XRP Ledger system as of October 4, 2012?

14 A. How many validators have been active
15 in the XRP Ledger? So, I don't know an exact
16 number. I suspect that the number of validators
17 on the XRP Ledger is between 100 and 200
18 validators.

19 That's a rough ballpark.

20 And on that day, there were
21 41 validators in the dUNL published at
22 VL.Ripple.com.

23 Q. Do you know how many dUNLs -- I'm
24 sorry, rephrase.

25 As of October 4, 2021, do you know how

1 [REDACTED] - Highly Confidential

2 many UNLs existed, besides the one that Ripple
3 published?

4 A. I don't know how many UNLs existed
5 beside the one that Ripple published.

6 Q. How can a validator on the ledger
7 change their UNL?

8 A. The validator on the ledger can change
9 the D -- UNL by changing its local state.

10 Q. Have you ever done it yourself?

11 A. I have not done it myself, no.

12 Q. Do you know how easy it is to do?

13 MR. SYLVESTER: Objection.

14 A. I don't know how easy or difficult it
15 is to do.

16 Q. Do you know if it can be done in the
17 space of a couple minutes?

18 A. I don't think it's relevant. I would
19 accept that it can be done quickly.

20 It poses certain challenges to the
21 system. If you're doing your -- if you're just
22 specifying your UNL, I think it's important, so
23 I'm agreeing with you that it's easy to change.

24 What should go on record, in my
25 opinion, is that this affects safety and live--

1 [REDACTED] - Highly Confidential

2 this may affect safety and liveness. So if --

3 Q. Okay.

4 A. -- if we as a network, we just specify
5 UNLs on our own and we don't get into sufficient
6 agreement, this sufficient overlap that I'm
7 describing in other parts of my report, it may
8 happen that we just don't play the same game, so
9 we'll get different views of the system and we
10 don't get to consensus.

11 Basically, you and me as honest nodes,
12 as honest validator operator nodes, as an
13 example, we are -- just don't have enough UNL
14 because we are not getting the same source of it
15 or we are not talking to each other to agree on
16 it.

17 There is the chance that if we do it
18 independently, as you're just describing it,
19 that we don't get -- that we can get consensus
20 priorities violated.

21 Q. Okay.

22 On page 26 of your report, in
23 answering E3, you wrote that, quote, If Ripple
24 disappears, there's a risk that universities
25 might cease to operate validators in the absence

1 [REDACTED] - Highly Confidential

2 of further funding.

3 And you're referring to universities
4 that participate in the University Blockchain
5 Research Institute?

6 A. University Blockchain Research
7 Initiative, yes. I do.

8 Q. Okay. Also for short, sometimes
9 called UBRI?

10 A. U-B-R-I, I call it, maybe UBRI, fair
11 enough.

12 Q. Are you making any assumptions in that
13 statement?

14 A. I'm making assumptions that, from my
15 experience as a university professor, is that
16 universities usually seek external funding, and
17 there are certain expenses, for manpower, for
18 computing power to ran validator nodes.

19 And to my understanding, the funding
20 of universities came -- of University Blockchain
21 Research Initiative came through Ripple.

22 And then, if Ripple disappears, I'm
23 saying there is a risk. I'm not quantifying the
24 risk. I am not sure even I am an expert to
25 quantify -- to quantify that risk. But I think

1 [REDACTED] - Highly Confidential

2 it's fair and assemble that there is a risk --

3 Q. Okay.

4 A. -- that the universities stop
5 operating their nodes.

6 Q. In citing that risk, did you assume
7 that the nine universities were receiving
8 funding from Ripple as of October 4, 2021?

9 MR. SYLVESTER: Objection.

10 A. I said Ripple has funded these
11 universities.

12 You know, what does it mean receiving
13 funding? Does -- is there -- was there a
14 payment on October 4, 2021? I didn't say that.

15 Q. Okay. Do you know if that's true or
16 not?

17 A. I don't know if that's true or not.

18 Q. Okay. Did you assume, in this part of
19 your report, that the nine universities have an
20 expectation of continued funding from UBRI
21 beyond October 4, 2021?

22 A. The implicit assumption here is that
23 it costs something to run the node. There are
24 no incentives from the protocol itself that
25 would fund this. For example, there are no

1 [REDACTED] - Highly Confidential

2 mining rewards or something similar.

3 So, it's -- cost certain money to have
4 the manpower or -- and the equipment to operate
5 this node. And, you know, if I am going to say
6 that there is no risk that these universities
7 eventually -- again, the word "eventually" where
8 we don't specify when this happens -- that they
9 stop because the funding stops. There is a risk
10 that this happens.

11 Q. Do you know how much it costs to run a
12 validator on the XRP Ledger?

13 A. I have some idea. So I think I saw
14 different numbers, like few -- there are numbers
15 of the cost of the -- of the node, which is in
16 thousands -- to my understanding, in thousands
17 of euros.

18 And if you run the fully -- full --
19 the validator with a full history, then the
20 storage can go to over 15 terabytes, so maybe
21 20 terabytes, roughly speaking, and this
22 blows -- this blows up the cost for running the
23 validator node.

24 Q. As part of your work on this case,
25 what communications have you had with anyone

1 [REDACTED] - Highly Confidential

2 from those nine UBRI universities?

3 A. I didn't have communications with
4 anyone from these nine UBRI universities.

5 Q. Okay. Do you have a factual basis to
6 state that those universities would cease
7 running a node if Ripple disappeared?

8 MR. SYLVESTER: Objection.

9 A. This is not what I stated. I stated
10 that there is a risk, and I tried to justify why
11 this risk exists.

12 Because universities usually rely on
13 external funding, there are no incentives in the
14 Ripple protocol to make -- to incentivize nodes
15 to -- to run the nodes, and this is the risk
16 that may happen. I'm not saying that it will
17 happen.

18 Q. I understand.

19 Other than in-protocol incentives, did
20 you do any work to consider what out-of-protocol
21 incentives UBRI universities might have to run a
22 validator node?

23 A. Out-of-protocol incentives for you --
24 UBRI, right, to run a validator node, could be
25 the funding that they got from Ripple and other

1 [REDACTED] - Highly Confidential

2 companies. This could be one incentive.

3 Q. Could it be anything else?

4 A. It could. It's -- you could have an
5 incentive to do research, to publish papers on
6 that. I didn't see -- I'm not saying these
7 don't exist. I never saw one.

8 Q. Okay.

9 A. I'm not saying these don't exist.

10 Q. In answering Question E3, you also
11 refer to four companies on the dUNL, Bitso,
12 COIL, Towo Labs and XRP Labs. And you state
13 that there's a risk that they could stop running
14 a validator, too. Correct?

15 A. Yes.

16 Q. Again, you're not saying it will
17 happen, you're saying that it's just -- it may
18 be a risk.

19 A. It may be risk. I think it relates to
20 Jeff, Alice and Bob example that you gave
21 before. So if -- if there is a -- there is a
22 risk that -- because of the connection --
23 business connections, that there is a -- there
24 is a risk that -- that if those companies depend
25 on funding by Ripple and it stops, it might be

1 [REDACTED] - Highly Confidential

2 going in the similar direction as we discussed
3 for university.

4 So I would say there is a risk. I'm
5 not saying it will happen, I'm saying it might
6 happen.

7 Q. Is it possible that those
8 four companies have independent business reasons
9 to support the XRP Ledger?

10 A. There is a possibility. Again, there
11 are no in-protocol incentives. It would be
12 considerably more transparent to reason about
13 independent economic and rational -- independent
14 economic players if you have in-protocol
15 incentives, if -- if there is something
16 intrinsic to the property -- to the protocol
17 that motivates you to continue what you're
18 doing.

19 Q. Did you speak with anyone at Bitso,
20 COIL, Towo Labs or XRPL Labs about their
21 incentives to run a validator?

22 A. I did not.

23 Q. Do you have -- as part of your work on
24 this case, did you investigate what products and
25 services those companies offer?

1 [REDACTED] - Highly Confidential

2 MR. SYLVESTER: Objection.

3 A. This was not a part of the questions
4 that I was asked to opine on.

5 Q. Were you curious to know if they
6 offered products or services that used the XRP
7 Ledger?

8 MR. SYLVESTER: Objection.

9 A. I was not curious to find out that. I
10 was answering to the questions I was asked.

11 Q. Let me direct you to your Appendix B
12 and B2. Briefly, in B2, you -- you present a
13 scenario in which you say that the XRP Ledger
14 could fail to guarantee liveness. Correct?

15 A. This is correct.

16 Q. Okay. And without going into detail
17 or reading what you wrote in B2, but I'm
18 referring here to your discussion in B2 and that
19 scenario, are you aware of whether the XRP
20 Ledger has any countermeasures to address such a
21 situation as the scenario you lay out in B2?

22 MR. SYLVESTER: Objection.

23 Go ahead.

24 A. The scenario that I am laying out in
25 B2 is the liveness analysis by Chase and

1 [REDACTED] - Highly Confidential

2 MacBrough. So this is the liveness analysis
3 done by Ripple employees.

4 So I didn't invent this. I'm
5 basically copying it from the paper that is --
6 if you look at the Ripple documentation and the
7 Ripple original white paper, it says it's
8 deprecated, in computer science terms, towards
9 this paper. And an external reader could assume
10 that this is an authoritative paper.

11 Q. Okay.

12 A. I did -- I did checks in the code to
13 understand whether this understanding that Chase
14 and MacBrough had when they published in 2018,
15 still matches, despite the software changes in
16 the last three years, at the moment I analyzed
17 the protocol, whether this is the case.

18 To best of my understanding, this is
19 still the case. So we can apply the analysis of
20 Chase and MacBrough.

21 Q. Okay. I'd like to show you --

22 A. I would like to finish my answer.

23 Q. Please do.

24 A. Yes. Because you're asking me to say,
25 like, this is my opinion. This is not my

1 [REDACTED] - Highly Confidential

2 opinion, this is the liveness analysis by Chase
3 and MacBrough.

4 So, I agree with that analysis.

5 You asked me whether there are certain
6 changes in the code, or actually, features in
7 the code that prevent this from happening.

8 So there are some features that are
9 doubled, detection of Byzantine validators in
10 the code. And these changes actually don't do
11 anything automatically.

12 So what they would do is, they would
13 alert the operator of human nodes.

14 Q. They would avert the --

15 A. Avert, if something happens, to the
16 best of my understanding, because they look at
17 they changes, they don't automatically try to
18 evict, potentially, Byzantine nodes from the --
19 from the system, from their UNL, for example,
20 but they would avert -- they would alert the
21 operator of the node. That's my best
22 understanding of what happens.

23 And then what it means for the -- in
24 the Chase/MacBrough analysis, it means that the
25 analysis stands. It's just that some human

1 [REDACTED] - Highly Confidential

2 operators, of which action would be required
3 later on, they would need to act on this
4 information.

5 The software, you know, maybe if it
6 detects, it raises a flag, but it doesn't do
7 more than that.

8 Q. Based on your understanding of the
9 Ledger's Byzantine validator detection measures,
10 do those measures make it less likely that
11 Scenario 2 -- that B2 in your report would
12 actually occur?

13 MR. SYLVESTER: Objection.

14 A. I'm not sure I can opine on that.

15 We would need to measure whether it's
16 less likely or not, whether they deter certain
17 participants from doing this.

18 I don't think we can come to that
19 conclusion.

20 There is no penalty to these nodes, so
21 I would say we cannot -- I -- I couldn't take
22 that standpoint, honestly.

23 MS. ZORNBERG: Okay. Let's go off the
24 record, just for efficiency's sake. And
25 we're still on time to get you out of here

1 [REDACTED] - Highly Confidential

2 by 6:00 o'clock. I want to take another
3 ten-minute break.

4 THE VIDEOGRAPHER: It is
5 5:00 o'clock p.m. We're going off the
6 record.

7 (Recess from 5:00 to 5:12.)

8 THE VIDEOGRAPHER: It is 5:12 p.m. We
9 are back on the record.

10 Q. Okay. Earlier today, you mentioned
11 having a close collaboration with an individual
12 named [REDACTED]

13 A. [REDACTED]

14 Q. [REDACTED] Correct?

15 A. Correct.

16 Q. Okay. Did you discuss your report
17 with him in this -- your report in this case
18 with him?

19 A. No.

20 Q. Are you aware of an article that
21 [REDACTED] co-authored in November 2020, titled
22 "Security Analysis of Ripple Consensus"?

23 A. I am.

24 Q. Have you read that article?

25 A. I did.

1 [REDACTED] - Highly Confidential

2 Q. Did you -- did you and [REDACTED] ever
3 discuss that article as he was writing it?

4 A. No.

5 Q. When did you read his article -- that
6 article?

7 A. I read the article, I believe the
8 first time he made it public. And I reread it
9 during the -- when I accepted the case, I reread
10 it to understand what -- in more details what
11 he's writing about. So I read it at least
12 twice.

13 Q. Okay. And one of the times you read
14 it was in connection with your work on this
15 case?

16 A. It is -- yeah, it was, yes.

17 Q. Okay. And the first time, do you --
18 do you also -- rephrase.

19 Do you recall that you also retweeted
20 [REDACTED] tweet of his -- of his article in 2020?

21 A. In November 2020?

22 Q. Actually, the tweet -- or retweet was
23 in December 2020.

24 A. I don't recall. I could trust you
25 that I did that.

1 [REDACTED] - Highly Confidential

2 Q. Okay. Let me show you [REDACTED] 17.

3 (2020 [REDACTED] article was marked [REDACTED]
4 Exhibit 17 for identification, as of this
5 date.)

6 Q. Okay. Dr. [REDACTED] is this the [REDACTED]
7 article from 2020 that you've just discussed
8 having read and then reread in connection with
9 your work on this case?

10 A. [REDACTED] yes, it is. It
11 appears to be, yes.

12 Q. Okay. Did you cite this among the
13 references of your report in this case?

14 A. I did not.

15 Q. Why not?

16 A. This paper shows an attack, which is
17 pointed out by [REDACTED] And then there
18 was a discussion -- in a sense, there was a --
19 an unofficial rebuttal by -- I believe it was
20 Brad Chase, I'm not sure. Definitely, somebody
21 closely connected to the -- to Ripple and to XRP
22 Ledger consensus protocol.

23 But they basically questioned the
24 attack. The attack is rather similar, if you
25 look at the -- if you look at the -- Figure 5 on

1 [REDACTED] - Highly Confidential

2 page 15.

3 The attack is somewhat similar to the
4 attack that I'm describing in Appendix B3, but
5 it actually applies to the different phase in
6 the protocol.

7 So I thought that Ripple's rebuttal in
8 this case that was offered in the discussion --
9 I think I'm referring to Twitter discussion and
10 some -- some -- basically comments of Ripple's
11 employees that could be fine with respect to
12 this report, I think they were grounded.

13 I don't think that the attack works.
14 My best understanding of Ripple system is that
15 this attack doesn't work as it's specified here.

16 So that that needs -- so it's just
17 that it doesn't work as it's described here. So
18 in that sense, I read it, and I didn't find
19 it -- because of this incorrection that I
20 perceived from my understanding of the protocol,
21 I didn't find it relevant to include it.

22 Because I don't think necessarily what's written
23 here is true.

24 Q. Okay.

25 Can I direct you to page 36 of your

1 [REDACTED] - Highly Confidential

2 report?

3 A. Yes.

4 Q. And -- and you mentioned page 15,
5 Figure 5 on page 15 of [REDACTED] 17?

6 A. Page 15, yes.

7 Q. Okay. So can you just -- you have a
8 Figure 5 also in your report. Are there
9 similarities between Figure 5 in your report and
10 Figure 5 in [REDACTED] report?

11 A. I report there are similarities, yes.
12 Here, it's similar in the sense that the setup
13 looks like, but the message is centered
14 different.

15 So Christian, basically mounts this
16 type of an attack at the different stage of the
17 protocol than what I did. So if you ask me, you
18 know, with this -- what is inspirational for my
19 attack maybe, was this -- I definitely read it
20 before I came up with the attack, but it's
21 different.

22 So it applies to -- there are
23 similarities, as I pointed out immediately, but
24 this applies to the different phase of the
25 protocol.

1 [REDACTED] - Highly Confidential

2 So my attack applies at a very
3 different phase of the protocol than Christian's
4 attack.

5 Q. Okay. Let me turn your attention now
6 to page 5 of your report, under "Governance."

7 So, in your report, you -- you note,
8 that Ethereum's development was funded using
9 proceeds of an ICO. Correct?

10 A. Correct.

11 Q. What was the ICO of Ethereum?

12 A. What?

13 MR. SYLVESTER: Objection.

14 A. What what?

15 Q. What was the ICO of Ethereum?

16 A. What was the ICO?

17 Let's see how I refer it to the -- in
18 order not to diverge from -- from what I wrote,
19 let's -- let's find when I mentioned the ICO and
20 just make sure that we are talking about the
21 same thing.

22 Q. So I'll -- I'll help you there. I can
23 direct you to page 18 --

24 A. 18.

25 Q. -- of your report.

1 [REDACTED] - Highly Confidential

2 Where, at the very bottom of 18, top
3 of 19, you reference 72 million ETH being
4 preallocated in the Genesis block?

5 A. I definitely agree with you, I'm just
6 trying to pinpoint the -- the line so --

7 Q. That line is at the very bottom of 18,
8 top of 19.

9 A. Yes, okay, I'm with you.

10 Q. Okay. So turning now to your chart on
11 page 5 of your report, under "Governance for
12 Ethereum," you write that Ethereum was 61 --
13 61.5 percent, about 10 percent owner controlled,
14 of today's supply.

15 I just want you to explain, please,
16 how did -- I want you to explain your math. How
17 did you come up with 61.5 percent?

18 A. It says 61.5 percent. If you, for a
19 moment, ignore what's in the brackets, we can
20 come back to that. It says 61.5 percent of
21 today's supply.

22 So today's supply can be estimated by
23 different means. It's actually -- for Ethereum,
24 it's difficult to pinpoint the exact supply, but
25 there are estimations, including on many

1 [REDACTED] - Highly Confidential

2 comparison sites, such as CoinMarketCap and
3 others, which would indicate roughly where the
4 supply stands.

5 And that number, 72 million, would be
6 61 percent -- 61.5 percent, roughly speaking --

7 Q. Okay.

8 A. -- of supply on that day.

9 Q. So how did you calculate 10 percent
10 owner controlled?

11 A. 10 percent owner controlled would
12 be -- let's go back.

13 What I think is 10 percent owner
14 control of today's supply. So you will take
15 today's supply. 10 percent of that should be
16 matching the 12 million Ether that I
17 nominally --

18 Q. Are you -- are you expressing --

19 A. -- referred to.

20 Q. Is it your belief that the -- the
21 launchers of Ethereum, the owners, initially
22 controlled a hundred percent and then sold some
23 of theirs -- percentage for money?

24 MR. SYLVESTER: Objection.

25 A. Could you restate, please?

1 [REDACTED] - Highly Confidential

2 Q. Do you have a view as to whether the
3 owners, as you're using that term to talk about
4 Ethereum blockchain, at any point owned a
5 hundred percent?

6 MR. SYLVESTER: Objection.

7 A. There is a moment on the Genesis
8 block. And the token 72 million Ether at the
9 moment of the Genesis block were 100 percent of
10 the supply at that time.

11 We can say that the game starts by --
12 at that moment where the allocation happened,
13 you could say that the development team
14 essentially may decide whatever it wants to
15 decide, right?

16 But it respects the informal
17 contractor, like from the ICO, that essentially
18 the bitcoin that were sent to their address, in
19 the procedure of the ICO, should be exchanged
20 for 72 million Ether. So that moment, there is
21 a genesis bulk -- bulk creation with the initial
22 distribution of coins.

23 Q. Why -- why, if your assignment in the
24 case was to compare the decentralization of
25 bitcoin, Ethereum and XRP Ledger, as of

1 [REDACTED] - Highly Confidential

2 October 4, 2021, why are you even talking about
3 owner control over -- you know, years ago, in
4 your chart on page 5?

5 A. So --

6 MR. SYLVESTER: Objection.

7 Go ahead.

8 A. Yes.

9 So owner control, in my review of the
10 literature, in one of the paper that we
11 discussed, which is the Sai paper, and
12 Exhibit [REDACTED] 4, where we discussed different
13 layers, and -- so I would refer you to page 12,
14 and Table 2 of the Sai paper, in the governance
15 layer, you asked me also about the
16 centralization factors Sai mentions in -- in
17 that paper.

18 So, I'm before, page 12. Table 2 at
19 the top of the page.

20 Q. Yeah, but in the methodology in your
21 report --

22 A. I didn't -- may I finish?

23 Q. Oh. Go ahead.

24 A. So, Sai has the owner control as a
25 centralization factor, and it's -- you know,

1 [REDACTED] - Highly Confidential

2 again, we are establishing here -- I was trying
3 to establish the methodology that would be
4 applicable, hopefully, beyond the three.

5 This is the way I approach things,
6 right? So if you call it the methodology should
7 be applicable to blockchains other than these
8 three.

9 Maybe if you switch to proof of stake
10 in any of the three, you know, you should be
11 still able to understand the dynamics and to
12 infer something about -- about the system,
13 right? So for that is --

14 Q. So was your --

15 A. Yeah, for that is -- owner control is
16 important because Sai mentions, he says once and
17 like layer, I call this facet. And because it
18 was part of the established methodology that we
19 discussed in details before, I'm evaluating this
20 owner control, and actually this owner control,
21 I took that from Sai.

22 Q. So, for purposes of owner control, are
23 you saying your methodology was not restricted
24 to looking at ledgers as of the date of your
25 report?

1 [REDACTED] - Highly Confidential

2 A. Owner control defines -- is defined in
3 Sai, and I think I repeat that -- let --
4 let's -- let's -- not because I know my report
5 better.

6 There is a point in which I cite Sai
7 in the methodology, and that should be --

8 Q. I'd like to restate my question --

9 A. Okay.

10 Q. -- rather than going into Sai.

11 My question is about the chart that
12 you wrote on page 5, and about your assignment
13 in this case.

14 Were you -- was your -- did your
15 methodology intend to compare bitcoin, Ethereum
16 and XRP Ledger as of the date of your report?

17 A. Yes. But this -- so, yes, but there
18 is this -- so if you look at page 11 of my
19 report, so in governance, which is introduced at
20 the very bottom of page 10, so there is this
21 governance aspect or -- or layer in Sai's
22 terminology.

23 Point C, owner control is defined as
24 measured by examining the total tokens
25 accumulated by the stakeholders in the early

1 [REDACTED] - Highly Confidential

2 adoption period. So since we discussed the Sai,
3 so you see that there is a time reference to the
4 early adoption period.

5 And since Sai as one of the
6 peer-reviewed papers which we discussed before,
7 which introduces the taxonomy of public
8 blockchain systems of this -- their
9 centralization, basically he defines it at that
10 point in time. I'm including that in my
11 methodology.

12 I also -- so -- so one other
13 justification is there -- there like --
14 informally people would -- you know, if there is
15 a fair distribution of tokens, if you have a
16 blockchain which didn't -- one who create the
17 blockchain didn't reserve the tokens for
18 himself, that's, in some sense, more equal or in
19 a sense -- so I see why Sai is doing that, why
20 he points out that you should not, as they call
21 it pre-mine the blockchain.

22 And -- and taking that as a
23 centralization measure, I see why this -- so I
24 agree with accepting that. But I'm not the only
25 one who proposes that, so at least Sai does.

1 [REDACTED] - Highly Confidential

2 And he refers -- so they refer to the
3 point -- so they really refer to the early
4 adoption period. If you just look through the
5 paper, they -- this is what owner control means.

6 Q. So, is it your view that even if
7 Ripple control -- let me rephrase.

8 Even if Ripple owned zero XRP today,
9 in deciding whether the XRP Ledger was
10 centralized or decentralized, you would still
11 look back to 2012 or 2013 to evaluate owner
12 control?

13 MR. SYLVESTER: Objection.

14 Go ahead.

15 A. Again, owner control as it was
16 defined, I'm accepting this as defined by other
17 scientific researchers. If we accept that this
18 is relevant, we would need to take it into
19 account.

20 It's also --

21 Q. Can you answer my question, though?
22 My question was --

23 A. Yes.

24 Q. -- if Ripple owned zero XRP today in
25 2021, would it be your view that to determine

1 [REDACTED] - Highly Confidential

2 the decentralization of the XRP Ledger, you
3 would still, under your methodology, need to
4 consider how much XRP Ripple owned back in 2013?

5 MR. SYLVESTER: Objection.

6 Go ahead.

7 A. Yes. I think what are you asking me
8 requires deeper understanding, but it's
9 relevant.

10 So I -- I don't know if you recall
11 that I described the attack on proof-of-stake
12 system where the old stakeholders can mount. I
13 didn't mention that it's called long-range
14 attack, but can go back in history to the point
15 where they control a lot of tokens.

16 So that's important, because if you
17 don't consider that in a proof-of-stake system,
18 which may be not relevant for three blockchain
19 systems we analyze here, but since this
20 methodology should be applicable to other
21 blockchains as well, this -- you would still
22 want to look at that, because the attacker could
23 go back in time to the point where it controlled
24 enough tokens to mount the attack and present
25 you with alternative history if the system

1 [REDACTED] - Highly Confidential

2 doesn't prevent this kind of attack.

3 Q. In the proof-of-stake system.

4 A. For example. We need to understand if
5 these are the only ones. So that's the part of
6 the methodology. As it's part of the
7 methodology, I'm putting all the -- all the
8 analyzed blockchains through that filter.

9 Q. Okay. Let me turn -- turn to a
10 question about bitcoin miners. Is there a point
11 when bitcoin miners will no longer be able to
12 receive mining awards?

13 A. So depends on how you define the
14 mining rewards. There are two rewards for
15 mining. One is the block reward, which halves
16 every 210,000 blocks, as I explain in my report.

17 There is another reward, which are
18 transaction fees. So whenever you submit a
19 transaction, you need to put some transaction
20 fee. And bitcoin miners will always be
21 collect -- assuming, again, no protocol changes,
22 simplify our life and to talk about the current
23 state of bitcoin software, is just runs after
24 2140, year 2140, where the block reward
25 disappears, but the mining reward is still there

1 [REDACTED] - Highly Confidential

2 because there are transaction fees.

3 If you see the distinction between the
4 mining reward and the block reward.

5 Q. So the mining rewards will run out
6 eventually for bitcoin?

7 A. No. They will -- mining -- miners are
8 rewarded by transaction fees and block reward.
9 They would run out from block reward, but they
10 would keep the transaction fees, which is part
11 of the mining reward.

12 Q. Okay. Is it -- I want to talk about
13 in-protocol incentives, which you define in your
14 report.

15 Is it your opinion that in-protocol
16 incentives are necessary to whether a blockchain
17 can be decentralized?

18 MR. SYLVESTER: Objection.

19 Go ahead.

20 A. Yes. So I think we made it clear that
21 the -- under the methodology that I'm presenting
22 here, we couldn't call them necessary.

23 But we would call a system that has
24 in-protocol incentives, in this -- so if there
25 are incentives to participants in the protocol

1 [REDACTED] - Highly Confidential

2 which are in -- in-protocol, we could claim,
3 under my methodology and under the standing of
4 researchers that I cited, that the system is
5 more decentralized than another one which
6 doesn't have this.

7 Q. So in your view, in-protocol
8 incentives are not necessary to
9 decentralization, but an in-protocol
10 decentralized system -- let me -- let me
11 rephrase.

12 So in your view, in-protocol
13 incentives are not necessary to whether a
14 blockchain is decentralized, but a blockchain
15 system with in-protocol incentives may be more
16 decentralized than others?

17 A. I think that fairly summarizes my
18 standpoint, yes.

19 Q. Okay.

20 In your definition of equal
21 opportunities, which is found on pages 15
22 through 16 of your report, do you assume that
23 there's a free market for computing power?

24 A. I do assume that there is a free
25 market for computing power.

1 [REDACTED] - Highly Confidential

2 Q. Does your application of equal
3 opportunities to bitcoin and Ethereum also
4 assume a free market for electricity?

5 A. It does.

6 Q. And does your application of equal
7 opportunities to bitcoin and Ethereum assume a
8 free market for Internet bandwidth?

9 A. We could say that it does, but that --
10 that aspect is considerably less of a challenge
11 with respect to two. If there is no free
12 market, for example, for computing power, and
13 that would be less of a challenge because the --
14 especially for bitcoin, the bandwidth is not
15 that big, but I -- I could agree, yes.

16 Q. Okay. So I think you just said it,
17 but would you agree that there actually is not a
18 free market throughout the globe for computing
19 power?

20 MR. SYLVESTER: Objection.

21 A. I did not say that.

22 Q. Is it your opinion that there is a
23 free market for computing power, in actuality?

24 A. I think --

25 MR. SYLVESTER: Objection. Beyond the

1 [REDACTED] - Highly Confidential

2 scope.

3 Go ahead.

4 A. Yes. So I didn't opine on this, and
5 I'm just saying assuming free market, there are
6 certainly properties.

7 Honestly, it's -- it's at which level
8 you zoom out and look at the game that we are
9 playing here. So, anyone can -- there is no
10 constraint that any, for example, nation or any
11 individual, that any organization could start
12 their own chip-producing facilities. It takes a
13 lot of knowledge.

14 It takes a lot of know-how, but
15 normally you're not prevented from doing that.
16 If you have that know-how, if you have the
17 resources, if you can produce your own chips,
18 you could do it.

19 You could do your own research
20 independently of others to advance the computing
21 power, and actually, we are doing that. I mean,
22 as a society, we are doing that. And nobody can
23 stop you, in that sense, from joining the game,
24 as I am discussing here.

25 Whether there is an ideal free market,

1 [REDACTED] - Highly Confidential

2 I guess, if -- you know, that in practice,
3 that's another thing that, you know, I don't
4 necessarily have an opinion on currently. I'm
5 assuming if there is, what are the rules of the
6 game?

7 Q. Your market assumes a free market for
8 computing power?

9 MR. SYLVESTER: Objection.

10 A. My --

11 Q. I misspoke. Your -- your definition
12 and application of equal opportunities to
13 bitcoin and Ethereum assumed a free market for
14 computing power?

15 A. This is what I said. So, because
16 you're trying maybe to -- to guide me to say
17 something that I don't necessarily plan to
18 say --

19 Q. You know what? I'll just point it out
20 in your report where -- a statement, see if you
21 still agree, and then -- and we'll stop it at
22 that.

23 On the top of page 16, you -- do you
24 acknowledge that for proof-of-work consensus,
25 assuming a free market for computing power,

1 [REDACTED] - Highly Confidential

2 existing participants cannot prevent new
3 participants from entering the system?

4 A. This is what I'm saying, if we assume
5 a free market for computing power, then existing
6 participants cannot prevent new participants
7 from entering the system.

8 MS. ZORNBERG: Okay. I think we're at
9 the 7-hour mark, so we're going to -- we're
10 going to stop here.

11 I'd like to put on the record that on
12 behalf of all three defendants in the case,
13 that we're going to request that a -- a
14 proper list that complies with the -- with
15 the Federal Rules of Procedure with Rule 26
16 be provided, of the materials considered by
17 Dr. [REDACTED] in preparing his report, and
18 we're going to reserve our right to
19 re-depose him once we get a proper exhibit
20 that complies with the rules.

21 MR. SYLVESTER: Well, we'll review his
22 testimony, and we reserve our rights as
23 well.

24 I have a few questions before we wrap
25 up for the day, which I'm happy to start

1 [REDACTED] - Highly Confidential

2 now.

3 EXAMINATION BY MR. SYLVESTER:

4 Q. Dr. [REDACTED] do you remember earlier
5 today, counsel asked you, Are you offering any
6 opinion in this case as to whether Ethereum is a
7 decentralized system?

8 A. I remember we discussed it.

9 Q. And throughout the day today, you've
10 testified as to methodology for the relative --
11 for assessing the relative decentralization of
12 bitcoin, Ethereum and the XRP Ledger, as you
13 were assigned to do in this case?

14 A. I did that. This is correct.

15 Q. Okay. And as part of your opinions
16 set forth in your expert report, you did apply
17 that methodology -- methodology to Ethereum.
18 Correct?

19 A. This is correct.

20 (Continued on following page to
21 include jurat.)

22

23

24

25

1 [REDACTED] - Highly Confidential

2 MR. SYLVESTER: Okay. That's all I
3 have.

4 MS. ZORNBERG: Okay. We're off the
5 record.

6 THE VIDEOGRAPHER: It is 5:37 p.m., we
7 are going off the record.

8 (Time noted: 5:37 p.m.)

9

10

11

12

13

14

15

[REDACTED] Ph.D.

16

Subscribed and sworn to before me

17

this day of 2021.

18

19

20

21

22

23

24

25

C E R T I F I C A T E

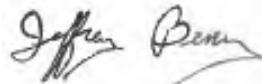
STATE OF NEW YORK)
) Ss.:
COUNTY OF NEW YORK)

I JEFFREY BENZ, a Certified Realtime Reporter, Registered Merit Reporter and Notary Public within and for the State of New York, do hereby certify:

That [REDACTED] Ph.D., the witness whose examination is hereinbefore set forth, was duly sworn by me and that this transcript of such examination is a true record of the testimony given by such witness.

I further certify that I am not related to any of the parties to this action by blood or marriage; and that I am in no way interested in the outcome of this matter.

IN WITNESS WHEREOF, I have hereunto set my hand this 20th of December, 2021.



JEFFREY BENZ, CRR, RMR

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

-----INDEX-----

WITNESS	EXAMINATION BY	PAGE
██████████ Ph.D.	MS. ZORNBERG	8
	MR. SYLVESTER	386

-----EXHIBITS-----

NUMBER	DESCRIPTION	PG	LN
Exhibit 1	Expert Report of ██████████ ██████████ Ph.D.,	67	6
Exhibit 4	Sai paper	129	25
Exhibit 5	Position paper "On the Future of Decentralized Computing"	176	16
Exhibit 8	Article titled "A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform"	214	12
Exhibit 9	Tweet from Neha Narula	223	13
Exhibit 10	"Quantifying Decentralization," Blockstack Summit 2017	277	9
Exhibit 11	Article Dated June 16, 2014, "Bitcoin Currency Could Have Been Destroyed by 51 Percent Attack,"	301	4
Exhibit 13	Document	75	5
Exhibit 13A	History Page	78	18
Exhibit 14	Report Citation	156	19
Exhibit 15	Document	158	15

NUMBER	DESCRIPTION	PG	LN
Exhibit 16	XRP chat	341	7
Exhibit 17	2020 [REDACTED] article	366	6

WITNESS DIRECTED NOT TO ANSWER:

Page 221

ERRATA SHEET

1
2 Case Name:

3 Deposition Date:

4 Deponent:

5	Pg.	No.	Now Reads	Should Read	Reason
6	_____	_____	_____	_____	_____
7	_____	_____	_____	_____	_____
8	_____	_____	_____	_____	_____
9	_____	_____	_____	_____	_____
10	_____	_____	_____	_____	_____
11	_____	_____	_____	_____	_____
12	_____	_____	_____	_____	_____
13	_____	_____	_____	_____	_____
14	_____	_____	_____	_____	_____
15	_____	_____	_____	_____	_____
16	_____	_____	_____	_____	_____
17	_____	_____	_____	_____	_____
18	_____	_____	_____	_____	_____
19	_____	_____	_____	_____	_____
20	_____	_____	_____	_____	_____

21 _____
Signature of Deponent

22 SUBSCRIBED AND SWORN BEFORE ME

23 THIS _____ DAY OF _____, 2021.

24 _____

25 (Notary Public) MY COMMISSION EXPIRES: _____

DEPOSITION ERRATA SHEET

Case Name: SEC V. RIPPLE
LABS, INC. ET AL

CIVIL ACTION NO. 20-CV-10832 (AT) (SN)

Deposition Date: DECEMBER 17, 2021

Deponent: [REDACTED]

Page	Line	Now Reads	Should Read	Reason
11	23	Don't get me for the accusation	Don't cite me on the accusation.	Transcript error
13	11	with maybe one hour, initial	for maybe one hour, initially	Transcript error
14	6	case	cases	Transcript Error
14	13	correct	correctly	Transcript Error
15	7	I'm interested	I was interested	Transcript error
22	19	very much freedom	a lot of freedom	Transcript error
24	15	number of quorums	size of quorums	Clarification
25	4, 5, 8, 15, 22, 23	Blockchain Protocols in the Wild	Blockchain Consensus Protocols in the Wild	Clarification
34	11,15	permission	permissioned	Transcript Error
34	12	call	called	Transcript error
46	<i>Lines 20-24 are confusing.</i>	So Adriaens would take the definition, you know -- definition. Take the sentence. There is no definition. Even Troncoso admits that there is no definition, no -- that's the motivation of their work, and they actually propose the definition.	So Adriaens misuses a sentence from Troncoso to say that Troncoso admits there is no definition, to which I say no, that is not the correct interpretation of Troncoso -- that's the motivation of their work, and they actually propose the definition.	Clarification
48	13	by	and buy	Transcript Error
57	13	This is actually similar to accept the ledger.	This is actually similar to XRP Ledger	Transcript Error
58	16, 18, 24	Byzantine full tolerance	Byzantine fault tolerance	Transcript Error
59	14	is relate	is related	Transcript Error

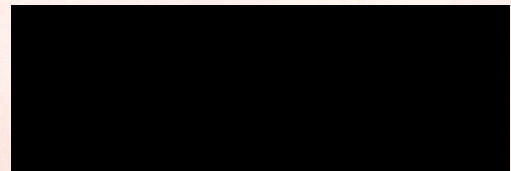
60	24	forge	fork	Transcript Error
60?	25	in order for that work on your network	in order for that to work on your network	Transcript Error
64	18	Ripple D	rippled	Transcript Error
65	13	very	wary	Transcript Error
73	22	my opinion with rippled 1.7.3.	my opinion assumes rippled 1.7.3.	Transcript error
83	6	I am not sure Pat	I am not sure if Pat	Transcript Error
84	15-16	treat it as a fixed line	treat it as fixed	Transcript Error
85	15-16	of the paper	of the report	Transcript Error
91	15	2021	2001	Transcript Error
93	2	Go on	Go	Transcript Error
95	11	There is a degree in innovation and entrepreneurship	There is a degree in innovation and entrepreneurship?	Clarification
95	22	I did not	I do not	Transcript error
98	16	And what the program committee does then is, that it reviews the papers submitted by other researchers.	And what the program committee does then is, it reviews the papers submitted by other researchers.	Transcript Error
98	23	oversee	oversees	Transcript Error
98	24	It	He/she	Clarification
100	2	set	said	Transcript Error
100	7	poses	implements	Clarification
103	5,6	permission	permissioned	Transcript error
103	7	coin mentors	inventors	Clarification
103	13	some cases, it could be in decentralized	in some cases, it could be decentralized	Transcript Error
103	22	permissionness	permissiveness	Transcript Error
104	12-13	or like orientation if IBM did – didn't work	or, like, orientation of IBM – it didn't work	Transcript Error
105	5,11	permission	permissioned	Transcript Error
106	12	asked it's	sked if it's	Transcript Error
107	4	has	had	Transcript error
108	4	Zurich	ETH Zurich	Clarification
113	3	if we	that we	Transcript Error
113	20	motiving	motivating	Transcript Error
113	25	important for people	important to people	Transcript Error
121	23	permission	permissioned	Transcript Error
122	17	didn't write	until I actually wrote	Clarification
122	25	is decentralized	as decentralized	Transcript Error
123	14	honesty	honest	Transcript Error
132	23	permission	permissioned	Transcript Error

134	25	permission	permissioned	Transcript Error
135	20 9	proprietors	properties	Transcript Error
140		would admit a system is decentralized, if it follows Troncoso definition.	would admit a system as decentralized, if it contradicts the Troncoso definition	Clarification
140	17	To my understanding, there is no definition of decentralization	To my understanding, there is no such definition of decentralization	Clarification
144	21	It would be if Ripple was actually	If Ripple was actually	Clarification
145	4	series	service	Clarification
145	18	opinion, as I stated my report, because of the	opinion, as I stated in my report, because the	Transcript Error/Clarification
148	8	depending	depend	Transcript Error
148	10	Newark	network	Transcript Error
149	8	such part	such party	Transcript Error
152	18	what a UNL does in Ripple code	which UNL to use	Clarification
153	16	ledger means the block -- XRP Ledger should be added to the blockchain	ledger means the block in the XRP Ledger -- which ledger should be added to the blockchain	Transcript Error
155	24	default Version Ripple dot -- this 1.7.3.	default Version rippled -- this 1.7.3.	Transcript Error
174	9	I tried this convey this is one possible test	I tried to convey this as one possible test	Transcript Error
181	23	permission	permissioned	Transcript Error
182	2	permission	permissioned	Transcript Error
182	4	inclusiveness	inclusiveness property	Clarification
182	22	report	paper	Clarification
187	7,8,11	permission	permissioned	Transcript Error
187	6	and we discuss this	and we discussed this	Transcript error
188	24	including this	inclusiveness	Clarification
189	19	takes	take	Transcript Error
190	4	on EPFL	at EPFL	Transcript error
191	16-17	with [REDACTED]	by [REDACTED]	Transcript error
191	17	it my head	it in my head	Transcript error
195	3	of the case	in the context of the case	Transcript error

196	12	I talk to SEC	I talked to SEC	Transcript error
202	14,17	permission	permissioned	Transcript Error
228	4,8	permission	permissioned	Transcript Error
229	10	struggling	struggling with	Transcript error
231	10	colleague	colleague who	Transcript error
234	7	coming	coming up	Transcript error
242	13	proof of state	proof of stake	Transcript Error
242	14	weight	weigh	Transcript Error
246	11,13	End function	AND function	Transcript Error/Clarification
246	18	network layer would probably be centralized.	network layer.	Transcript Error
252	3	partition	partitioned	Transcript error
252	4	to say unreliable network	to say this is "unreliable network	Clarification
253	13	official Lynch-Patterson consultancy possibility	Fischer-Lynch-Patterson consensus impossibility	Clarification
259	23	that favor in the	that favor safety in the	Clarification
260	8	that was opted	that opted for liveness/availability	Clarification
261	21	it tends	tends	Transcript error
263	5	That	That would be	Transcript error
263	17	role	rule	Transcript Error
263	20	forward network	forward progress	Transcript Error/Clarification
267	8	bettering the ability	better readability	Clarification
272	8	my miners with some	my miners and with some	Clarification
273	15	faulty	faulty nodes	Clarification
273	22	that and proof of work	that for proof of work	Transcript error
277	21	or a	of a	Transcript Error
282	9	relay	relate	Transcript Error
291	14	reserve	satisfy	Clarification
300	8	single people	single person	Transcript error
302	18	the guardian	the Guardian	Transcript Error
305	15	U.S. governments	U.S. government	Transcript Error
309	8	0.4	0.14	Clarification
310	18	mine	mined	Transcript Error
311	3-4	in protocol	in-protocol	Transcript Error
311	11	could not opt to	could opt to	Clarification
312	6-9	It's not correct that if a mining pool can opt which transactions to include, there are	It's not correct that if a mining pool can opt which transactions to	Clarification

		other mining pools that can opt to include the transaction	include that the Nakamoto coefficient would be 1, because there are other mining pools that can opt to include the transaction	
312	24	cash	hash	Transcript Error
336	20	use cases	use case	Transcript Error
338	8	pass from causal definition	go from the basic definition	Clarification
338	11	inclusive	inclusive systems	Clarification
338	13	on a	as	Transcript Error
339	21	Ripple D	rippled	Transcript Error
349	6	4.1	41	Clarification/Transcript Error
350	24, 25	natural cooperators	operators of XRP Ledger nodes	Clarification
353	13	UNL	UNL overlap	Clarification
354	18	ran	run	Transcript Error
355	2	and assemble	to say	Clarification
362	15	avert	alert	Transcript Error

Date: 20.5.2022



Brittany Shantez Goodman

